Cisco TelePresence Video Communication Server

Administrator Guide

D14049.09

December 2010

Software version: X6

Contents

Contents 2

About the Cisco TelePresence Video Communication Server (Cisco VCS) 16

Cisco VCS base applications 16

Cisco VCS Control 16

Cisco VCS Expressway™ 16

Standard features 17

Optional features 17

FindMe™ 18

Device Provisioning 18

Dual Network Interfaces 18

About this guide 19

Typographical conventions 19

Installation and initial configuration 19

Using the web interface 20

Required fields 20

How page navigation is shown in this guide 20

Supported browsers 20

Using the command line interface (CLI) 21

Command types 21

Web page features and layout 22

What's new in this version? 24

Enhanced authentication policy 24

External policy services 24

Secure communication between cluster peers 24

View registrations and calls across a cluster 24

Client-initiated connection management 24

Starter Pack enhancements 24

User interface language packs 24

Enhanced online help 25

Cisco VCS unit LCD panel 25

Multiple remote syslog servers 25

- SNMPv3 support 25
- Web interface 25

Overview and status information 26

- Status overview 26
- System information 27
- Ethernet status 28
- IP status 29
- Resource usage 30
- Registration status 30
  - Registrations by device 30
  - Registrations by alias 31
  - Registration history 32
  - Registration details 33
- Call status 33
  - Call status 33
  - Call history 34
  - Call summary 34
  - Call details 35
  - Call media details 35
- Search history 35
  - About searches 35
  - Search history list 36
  - Search details 36
- Local Zone status 37
- Zone status 37
- Link status 38
- Pipe status 38
- Policy service status 38
- TURN relays status 39
- Presence 39
  - Presence publishers 39
  - Presence presentities 40
  - Presence subscribers 40

OCS Relay status 41

Provisioning status 41

Provisioning server 41

Phone book server 42

Warnings 42

Hardware status 42

Event Log 42

Configuration Log 44

Cisco VCS unit front panel 45

Network and system settings 46

Configuring IP settings 46

Configuring Ethernet settings 47

Configuring DNS settings 48

Configuring Quality of Service settings 49

Configuring system name and access settings 49

Configuring SNMP settings 50

Configuring time zone and NTP server settings 52

Configuring the Login page 53

Configuring external manager settings 53

Configuring logging levels 54

Event Log levels 54

Remote logging 55

Protocols 56

About H.323 56

Using the Cisco VCS as an H.323 gatekeeper 56

H.323 endpoint registration 56

About SIP 56

Cisco VCS as a SIP registrar 57

Cisco VCS as a SIP proxy server 58

Proxying registration requests 58

Cisco VCS as a SIP Presence Server 59

H.323 configuration 59

SIP configuration 60

Configuring SIP domains 62

Configuring SIP and H.323 interworking 62

Searching by protocol 62

Enabling SIP endpoints to dial H.323 numbers 63

Registration control 64

About registrations 64

Finding a Cisco VCS with which to register 64

Registrations on a Cisco VCS Expressway 64

MCU, gateway and Content Server registration 65

Configuring registration restriction policy 65

Registering aliases 66

H.323 66

SIP 66

Attempts to register using an existing alias 67

Blocking registrations 67

Removing existing registrations 67

Re-registrations 67

About Allow and Deny Lists 68

Configuring the registration Allow List 68

Configuring the registration Deny List 69

Device authentication 70

About device authentication 70

Authentication Policy 70

Authentication mechanism 70

Authentication Policy configuration options 71

Zone-level Authentication Policy 71

Subzone-level Authentication Policy 73

SIP authentication trust 74

Device authentication configuration 75

Authentication database 75

Endpoint credentials used for authentication 75

Device authentication using LDAP 75

Authentication process 75

LDAP server settings 76

Device LDAP schemas 77

Authentication using a local database 78

Authenticating with external systems 78

Zones and neighbors 79

About your video communications network 79

Example network diagram 79

Structuring your dial plan 80

Flat dial plan 80

Structured dial plan 80

Hierarchical dial plan 80

About the Local Zone and subzones 81

Bandwidth management 81

Local Zone searches 81

About zones 82

Default Zone 82

Zone configuration 82

Configuring neighbor zones 83

Configuring traversal client zones 86

Configuring traversal server zones 88

Configuring ENUM zones 91

Configuring DNS zones 92

Zone configuration: advanced settings 93

Zone configuration: pre-configured profile settings 98

TLS certificate verification of neighbor systems 99

Clustering and peers 100

About clusters 100

About the configuration master 101

Secure communication between peers 101

Alternates 101

Setting up a cluster 101

Maintaining a cluster 102

Cluster name 102

Cluster pre-shared key 102

Setting configuration for the cluster 102

Adding and removing peers from a cluster 102

Changing the master peer 102

Monitoring the status of the cluster 103

Configuration that is not replicated across a cluster 103

Troubleshooting cluster replication problems 104

Managing clusters and peers 105

Sharing registrations across peers 105

Sharing bandwidth across peers 105

Cluster upgrades and downgrades 106

Cluster backup and restore 106

Clustering and FindMe 106

Clustering and Presence 107

Clustering and Cisco TMS 107

About the Cluster Subzone 107

Neighboring the local Cisco VCS to another Cisco VCS cluster 108

TMS Agent replication status 109

Dial plan and call processing 110

Call routing process 110

How the Cisco VCS determines the destination of a call 110

About the Cisco VCS's directory service 112

About hop counts 112

Configuring hop counts 112

About transforms and search rules 112

Transforms 113

Search rules 113

Dial plan configuration 113

About the fallback alias 114

About pre-search transforms 115

Pre-search transform process 115

Configuring pre-search transforms 115

Search and zone transform process 117

Configuring search rules 118

Example searches and transforms 120

Filter queries to a zone without transforming 121

Always query a zone with original alias (no transforms) 121

Query a zone for a transformed alias 122

Query a zone for original and transformed alias 123

Query a zone for two or more transformed aliases 124

Stripping @domain for dialing to H.323 numbers 125

Transforms for alphanumeric H.323 ID dial strings 127

Allowing calls to IP addresses only if they come from known zones 129

Configuring policy services 129

About Call Policy 131

Configuring Call Policy 131

Configuring Call Policy rules using the web interface 133

Configuring Call Policy using a CPL script 134

Configuring Cisco VCS to use the Cisco TelePresence Advanced Media Gateway 134

Configuring the Cisco VCS Control 135

Usage features and limitations 135

Configuring Cisco AM GW policy rules 135

Dialable address formats 137

Dialing by IP address 137

Dialing by H.323 ID or E.164 alias 137

Dialing by H.323 or SIP URI 138

Dialing by ENUM 138

IP dialing 138

Calls to unknown IP addresses 138

About URI dialing 139

URI dialing without DNS 139

URI dialing via DNS 140

URI resolution process using DNS 141

URI dialing via DNS for outgoing calls 142

URI dialing via DNS for incoming calls 144

URI dialing and firewall traversal 146

About ENUM dialing 146

ENUM dialing process 146

Enabling ENUM dialing 147

ENUM dialing for outgoing calls 147

Zone configuration for ENUM dialing 148

ENUM dialing for incoming calls 150

Configuring DNS servers for ENUM and URI dialing 151

Configuring a zone for incoming calls only 151

Call signaling configuration 151

Identifying calls 152

Disconnecting calls 154

Disconnecting a call using the web interface 154

Disconnecting a call using the CLI 154

Limitations when disconnecting SIP calls 154

Bandwidth control 156

About bandwidth control 156

Example network deployment 156

Bandwidth configuration 157

About downspeeding 158

About subzones 158

Default links between subzones 158

About the Traversal Subzone 158

About the Default Subzone 159

Configuring subzones 159

Configuring subzone membership rules 160

Applying bandwidth limitations to subzones 162

Links and pipes 163

Configuring links 163

Default links 164

Configuring pipes 164

Applying pipes to links 165

Bandwidth control examples 166

Firewall traversal 169

About firewall traversal 169
Expressway solution 169
How does it work? 169
Cisco VCS as a firewall traversal client 170
Cisco VCS as a firewall traversal server 170
Configuring traversal server zones 170
Configuring other traversal server features 170
Quick guide to Cisco VCS traversal client - server configuration 170
Firewall traversal protocols and ports 172
Expressway process 172
H.323 firewall traversal protocols 172
SIP firewall traversal protocols 172
Ports for initial connections from traversal clients 172
Default port summary 173
TURN ports 173
Ports for connections out to the public internet 174
Firewall traversal and authentication 174
Authentication and NTP 176
Firewall traversal and Dual Network Interfaces 176
Firewall configuration 176
Configuring traversal for endpoints 177
Configuring traversal server ports 178
About ICE and TURN services 178
About ICE 178
About TURN 179
TURN relay server 179
Configuring TURN services 179
TURN relay status information 180
Applications 181
Conference Factory 181
Conference creation process 181
About Presence 182
Presence Server 183

Presence User Agent (PUA) 183

Configuring Presence 185

OCS Relay 186

Configuring a connection between the Cisco VCS and the OCS 187

About FindMe™ 187

How are devices specified? 188

FindMe process overview 188

Who must do what before FindMe can be used? 188

Recommendations when deploying FindMe 189

Example 189

Configuring FindMe 189

Searching for FindMe users 191

About provisioning (Starter Pack) 191

Starter Pack 191

Device authentication 192

Phone book support 192

Configuring provisioning 192

Maintenance 193

About upgrading software components 193

Cisco VCS software components 193

Prerequisites 193

Backing up before upgrading 194

Upgrading and option keys 194

Installing and rebooting 194

Upgrade procedure 194

Upgrading using secure copy (SCP/PSCP) 195

Option keys 196

Adding option keys using the web interface 196

Adding option keys using the CLI 197

About security certificates 197

Managing security certificates 198

Advanced account security 199

Prerequisites 199

Cisco VCS functionality: changes and limitations 199

Configuring language settings 200

Changing the language 200

Installing language packs 200

About login accounts 200

Account authentication 201

Administrator accounts 201

User accounts 201

Root accounts 202

Configuring login account authentication 202

Account authentication using LDAP 202

Login history 204

Root account 204

Resetting an administrator or root password 205

Resetting user account passwords 205

Configuring administrator accounts 205

Password strength 206

Configuring administrator groups 207

Configuring user accounts 208

Principal devices (Starter Pack only) 209

Configuring user groups 211

Backing up and restoring Cisco VCS data 211

Limitations 212

Creating a backup 212

Restoring a previous backup 213

Creating a system snapshot 213

Incident reporting 213

Incident reporting warning: privacy-protected personal data 214

Sending incident reports automatically 214

Sending incident reports manually 214

Viewing incident reports 215

Incident report details 215

Checking the effect of a pattern 216

Locating an alias 216

Port usage 217

- Local VCS inbound ports 218
- Local VCS outbound ports 218
- Remote listening ports 218

Restarting 218

- Restarting using the web interface 219

Rebooting 219

- Rebooting using the web interface 219

Shutting down 220

- Shutting down using the web interface 220
- Shutting down using the CLI 220

Reference material 221

Software version history 222

- X5.2 222
- X5.1 223
- X5 225
- X4 228

About Event Log levels 230

- Event Log format 230
- Administrator and FindMe user events 230
- Message details field 231
- Events and levels 233

CPL reference 240

- CPL address-switch node 240
- otherwise 242
- not-present 242
- location 243
- rule-switch 243
- proxy 244
- reject 244
- Unsupported CPL elements 244
- CPL examples 245

LDAP configuration for device authentication 252

- Downloading the H.350 schemas 252
- Configuring a Microsoft Active Directory LDAP server 252
- Configuring an OpenLDAP server 254

DNS configuration examples 257

- Verifying the SRV record 257
- Microsoft DNS server 257
- BIND 8 & 9 257

Changing the default SSH key 258

- Default SSH key warnings 258
- Standalone Cisco VCS 258
- Clustered Cisco VCS 258

Restoring default configuration 259

- Configuration items reset by DefaultValuesSet level 3 259
- Configuration items reset by DefaultValuesSet level 2 260

Password encryption 262

- Maximum length of passwords 262

Pattern matching variables 263

Port reference 265

Regular expressions 271

Supported characters 273

- Case sensitivity 273

TMS Agent 274

- FindMe 274
- Device Provisioning 274
- TMS Agent account passwords 275

TMS Agent passwords 275

- TMS Agent LDAP and replication accounts 275
- Cisco VCSs managed by Cisco TMS 275
- Cisco VCSs not managed by Cisco TMS 276

What are traversal calls? 277

Warnings list 278

Bibliography 283

Glossary 286

Legal notices 294

Intellectual property rights 294

Copyright notice 294

Patent information 294

Disclaimers and notices 295

About the Cisco TelePresence Video Communication Server (Cisco VCS)

The Cisco TelePresence Video Communication Server (Cisco VCS) enhances the video experience and provides seamless communication between SIP and H.323 devices utilizing IETF and ITU standards. The Cisco VCS is the center of the video communication network, and connects all H.323 and SIP endpoints, infrastructure, and management devices. It provides unrivaled scalability and redundancy to video communications, and is integral to Cisco interoperability with unified communications and Voice over IP systems.

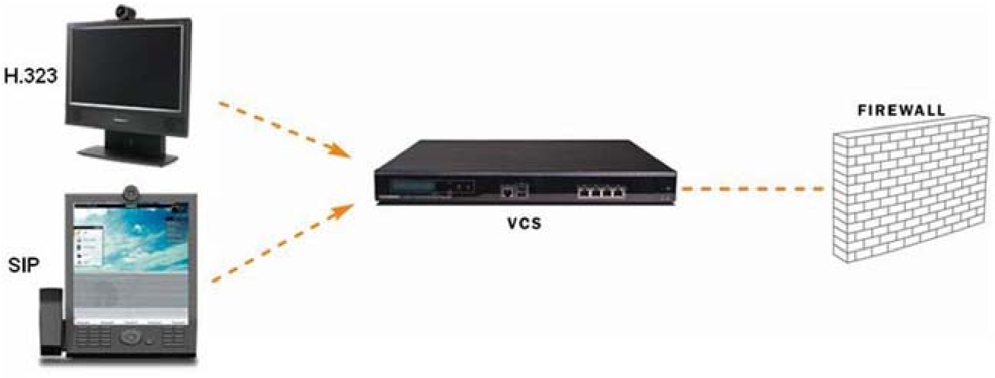
The Cisco VCS can be deployed with either the Control application or the Expressway™ application, with various optional packages including FindMe™, Dual Network Interfaces and Device Provisioning.

Cisco VCS base applications

The Cisco VCS is available with alternative base applications as described below.

Cisco VCS Control

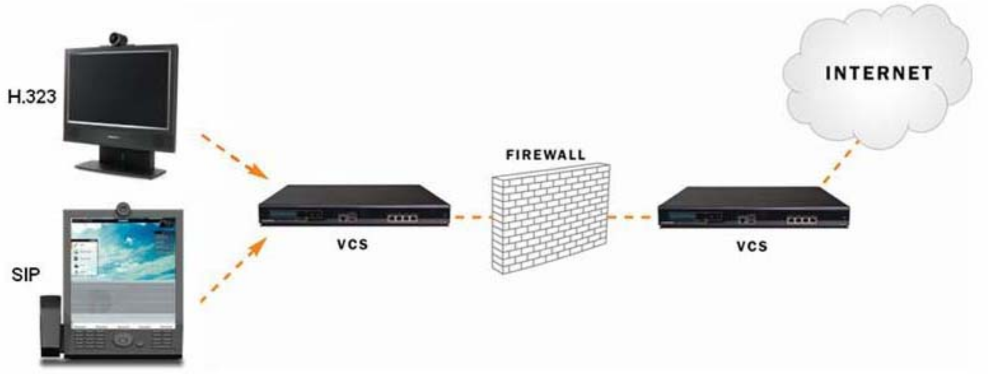
The Cisco VCS Control provides internal video control and administration for all SIP and H.323 devices. It is normally deployed within your wide area network with endpoints that are behind the same firewalls or NAT devices. The Cisco VCS Control replaces the need to have separate H.323 gatekeeper, SIP registrar and H.323 - SIP gateway servers.



Cisco VCS Expressway™

The Cisco VCS Expressway provides standards-based firewall traversal for SIP and H.323 devices allowing secure firewall traversal of any firewall or NAT device. As well as all the functionality of a Cisco VCS Control, it also provides registration of traversal-enabled devices and can act as a standards-based TURN server.

The Cisco VCS Expressway is normally deployed outside of your firewall or within the DMZ.



Standard features

The Cisco VCS has the following standard features:

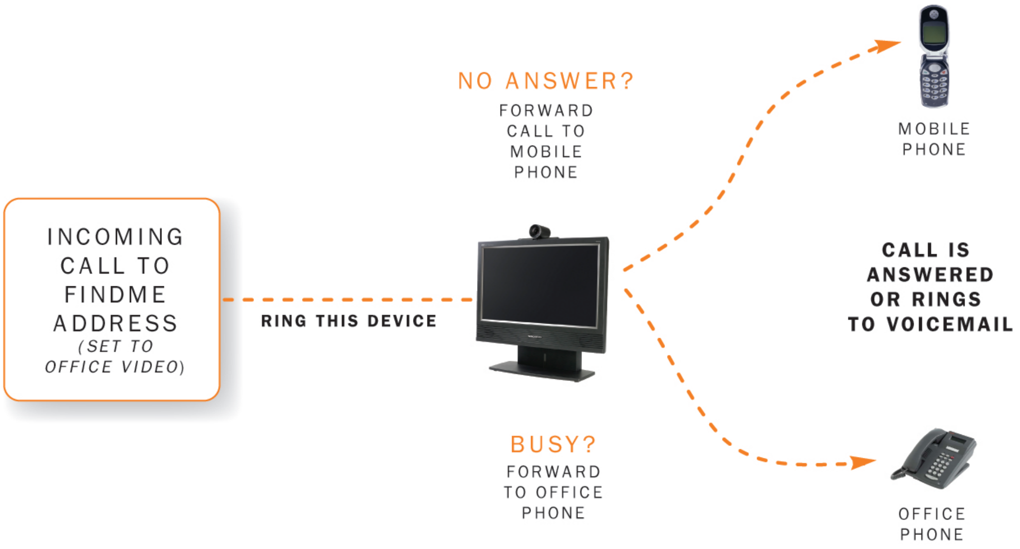
- 2500 endpoint registrations
- H.323 gatekeeper
- SIP Proxy/Registrar
- SIP Presence Server
- SIP Presence User Agent
- SIP and H.323 support, including SIP/H.323 gatewaying
- IPv4 and IPv6 support, including IPv4/IPv6 gatewaying
- QoS tagging
- Bandwidth management on both a per-call and a total usage 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 100 traversal calls
- 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 Cisco VCS or be neighbored with other systems such as Cisco VCSs, Border Controllers, gatekeepers and SIP proxies
- n+1 redundancy, can be part of a cluster of up to 6 Cisco VCSs for increased capacity and redundancy
- 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
- Can be managed with Cisco TelePresence Management Suite (Cisco TMS) 12.5 or later
- AD authentication for administrators of the Cisco VCS
- Pre-configured defaults for:
  - Cisco Unified Communications Manager neighbor zones
  - Cisco TelePresence Advanced Media Gateway
  - Microsoft Office Communications Server (OCS) 2007 neighbor zones
  - Nortel Communication Server neighbor zones
- Embedded setup wizard using a serial port for initial configuration
- System administration using a web interface or RS-232, Telnet, SSH, and HTTPS

Optional features

The following features are available on the Cisco VCS by the purchase and installation of the appropriate option key:

FindMe™

A unique industry solution that gives individual video users a single alias on which they can be contacted regardless of location. Users have the ability to log on to a Web-based interface and control where and how they are contacted. The FindMe feature also includes support for Microsoft Office Communications Server (OCS) 2007, enabling FindMe aliases to register as Microsoft Office Communicator (MOC) clients, and MOC clients to view the presence status of FindMe aliases.



Device Provisioning

The Device Provisioning option key allows Cisco VCS to provision endpoints with configuration information on request and to supply endpoints with phone book information. (Endpoints including Movi v2.0 or later, and E20 v2.1 or later can request to be provisioned.) All configuration and phone book information is managed in Cisco TMS, and distributed to the clients through the TMS Agent running on the Cisco VCS. The TMS Agent on the Cisco VCS also provides Cisco TMS with the provisioned client’s status.

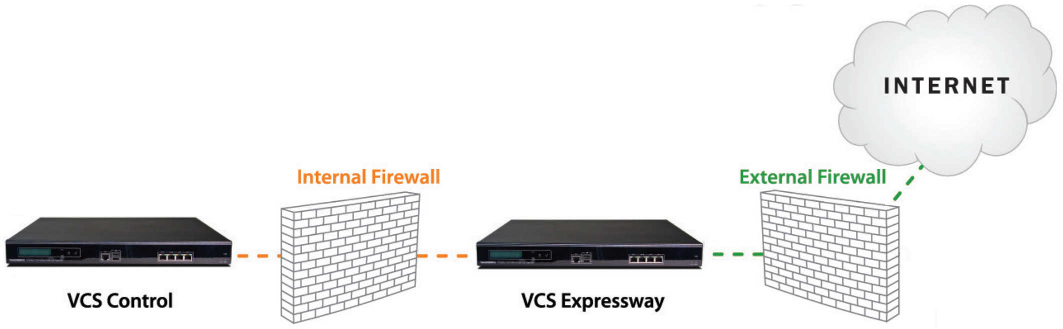
There is no configuration associated with Device Provisioning on the Cisco VCS – it is either on or off, depending on whether or not the option key is installed. See the Cisco TMS documentation and the *Provisioning* deployment guide [26].

Dual Network Interfaces

Enables the LAN 2 Ethernet port on the Cisco VCS Expressway, allowing you to have a secondary IP address for your Cisco VCS.

This option also includes support for deployments where a Cisco VCS Expressway is located behind a static NAT device, allowing it to have separate public and private IP addresses.

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



About this guide

This Administrator Guide is provided to help you make the best use of your Cisco VCS.

Your approach to this documentation depends on what you want to do and how much you already know. The Administrator Guide has been divided into several sections, providing conceptual, configuration and reference information about the various features and capabilities of the Cisco VCS.

This Administrator Guide describes a fully equipped version of the Cisco VCS. Your version may not have all the described extensions installed.

Our main objective with this Administrator Guide is to address your goals and needs. Please let us know how well we succeeded!

Typographical conventions

Most configuration tasks on the Cisco VCS can be performed by using either the web interface or a command line interface (CLI).

This guide mainly describes how to use the web interface. Some Cisco VCS features are only available through the CLI and these are described as appropriate, including the relevant CLI command.

In this guide, instructions for performing a task using the web interface are shown in the format:

- **Menu > Submenu**

followed by the **Name** of the page that you will be taken to.

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

- **xConfiguration <Element> <SubElement>**
- **xCommand <Command>**

Installation and initial configuration

Full installation and initial configuration instructions for the Cisco VCSare contained in the *Cisco VCS Getting Started Guide* [28].

Using the web interface

Configuration of the Cisco VCS 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**.
3. Enter a valid administrator **Username** and **Password** and click **Login** (see the Login accounts section for details on setting up administrator accounts). You are presented with the **Overview** page.

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

A command line interface is also available.

Required fields

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

How page navigation is shown in this guide

Instructions for navigating the web interface are shown in the format **Menu option 1 > Menu option 2** followed by the **Name** of the page that you are taken to in order to perform a task.

Supported browsers

The Cisco VCS web interface is designed for use with Internet Explorer 6 or later, and Firefox 2 or later. It may work with Opera and Safari, but you could encounter unexpected behavior.

Javascript and cookies must be enabled to use the Cisco VCS web interface.

Using the command line interface (CLI)

The Cisco 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. Access using Telnet can also be enabled. These settings are controlled on the System administration page.

To use the CLI:

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

Command types

Commands are divided into the following groups:

- **xStatus**: these commands return information about the current status of the system. Information such as current calls and registrations is available through this command group.
- **xConfiguration**: these commands allow you to add and edit single items of data such as IP address and zones.
- **xCommand**: these commands allow you to add and configure items and obtain information.
- **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.

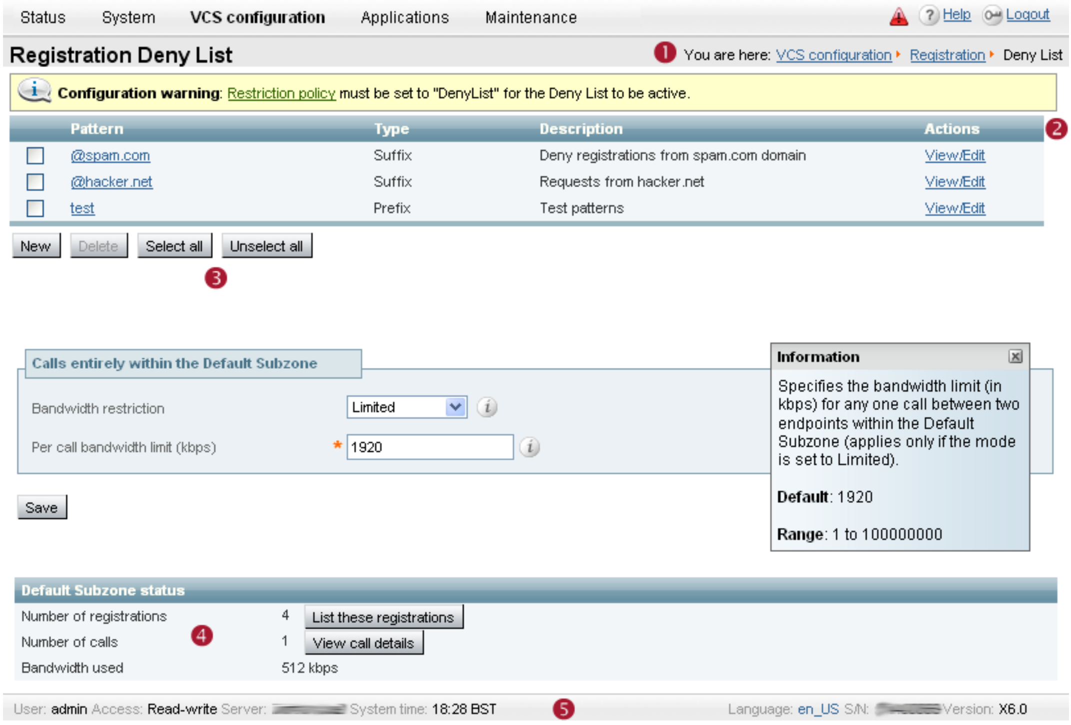
Note that:

- 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.

See the *Video Communication Server Command Reference* [40] for a full description of the commands available on the Cisco VCS.

Web page features and layout

This section describes the features that can be found on some or all of the web interface pages.



Registration Deny List

You are here: VCS configuration ▸ Registration ▸ Deny List

Configuration warning: Restriction policy must be set to "DenyList" for the Deny List to be active.

	Pattern	Type	Description	Actions
□	@spam.com	Suffix	Deny registrations from spam.com domain	View/Edit
□	@hacker.net	Suffix	Requests from hacker.net	View/Edit
□	test	Prefix	Test patterns	View/Edit

New | Delete | Select all | Unselect all

Calls entirely within the Default Subzone

Bandwidth restriction: Limited

Per call bandwidth limit (kbps) *: 1920

Save

Information

Specifies 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

Range: 1 to 100000000

Default Subzone status

Number of registrations	4	List these registrations
Number of calls	1	View call details
Bandwidth used	512 kbps	

User: admin Access: Read-write Server: [redacted] System time: 18:28 BST Language: en_US S/N: [redacted] Version: X6.0

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 warning	⚠	This icon appears on the top right corner of every page when there is a system warning in place. Click on this icon to go to the Warnings page which gives information about the warning and its suggested resolution.
Help	?	This icon appears on the top right corner of every page. Clicking on this icon opens a new browser window with help specific to the page you are viewing. It gives an overview of the purpose of the page, and introduces any concepts configured from the page.
Log out	🔑	This icon appears on the top right corner of every page. Clicking on this icon ends your administrator session.
Field level information	i	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.

Page element		Description
Information bar	ℹ	The Cisco 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	❷	Click on column headings to sort the information in ascending and descending order.
Select All and Unselect All	❸	Use these buttons to select and unselect all items in the list.
Mandatory field	*	Indicates an input field that must be completed.
Status	❹	On configuration pages, this section shows you the current status of the items you are configuring. Note that some configuration changes require a restart to take effect, so if you have changed the configuration but not yet restarted this shows the existing (unchanged) status.
System Information	❺	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, hardware serial number and Cisco 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.

What’s new in this version?

The new features introduced in this release of Cisco VCS software are described below.

Enhanced authentication policy

Authentication policy can now be applied at the zone and subzone levels. It controls how the Cisco VCS authenticates incoming messages from that zone or subzone and whether those messages are rejected or are subsequently treated as authenticated or unauthenticated within the Cisco VCS.

This provides increased flexibility and allows system administrators to:

- control registrations via subzones; this allows, if required, a combination of authenticated and unauthenticated endpoints to register to the same Cisco VCS
- limit the services available to unregistered or unauthenticated endpoints and devices
- cater for endpoints from third-party suppliers that do not support authentication within their registration mechanism through a "treat as authenticated" setting

External policy services

The Cisco VCS can be configured to use external policy services to manage its registration and call policies.

This is particularly suitable for large-scale deployments where policy decisions can be managed through an external, centralized service rather than by configuring policy rules on the Cisco VCS itself.

Secure communication between cluster peers

The Cisco VCS uses IPsec (Internet Protocol Security) to enable secure communication between each cluster peer. Authentication is carried out through the use of a pre-shared access key (configured on the **Clustering** page).

View registrations and calls across a cluster

You can now view all of the registrations and calls across a cluster from any one of the peers in the cluster. A **Peer** column on the registrations and calls status pages identifies the relevant peer.

Client-initiated connection management

The Cisco VCS has implemented support for RFC 5626 (known as "SIP Outbound"). This allows a UA to route calls when a peer in a cluster has failed, and also allows a UA to close all listening ports ensuring all calls can only be routed via their existing (authenticated, authorized) connection to the Cisco VCS.

Starter Pack enhancements

- The Cisco VCS Starter Pack Express supports device provisioning for E20 and Ex series endpoints.
- Additional call license option keys can be added to extend the default limit of 5 concurrent calls.

User interface language packs

Multiple language support has been enabled on the Cisco VCS's web interface. Language packs will be made available for download in the future. Contact your Cisco support representative for more information on supported languages.

Enhanced online help

The context-sensitive help available through the Help link at the top of every page on the web interface now contains additional conceptual and reference information. The help is fully searchable and also includes a table of contents to aid navigation between topics.

Cisco VCS unit LCD panel

The LCD panel on the front of the Cisco VCS hardware unit can be configured to show additional status information. It can display the system name, all IP addresses, warnings, and the number of current traversal calls, non-traversal calls and registrations.

Multiple remote syslog servers

The Cisco VCS now supports multiple remote syslog servers.

SNMPv3 support

The Cisco VCS now supports secure SNMPv3 authentication and encryption.

Web interface

- The **VCS configuration > search rules** menu has been renamed as **VCS configuration > Dial plan**. It contains the following submenu items:
  - **Configuration**: used to configure how the Cisco VCS routes calls in specific call scenarios.
  - **Transforms**: the pre-search transforms configuration option previously found directly under the **VCS configuration** main menu.
  - **Search rules**: used to configure search rules.
  - **Policy services**: used to define the policy services that can be used as a target of a search rule.
- The **Overview** top-level menu option has been removed and the **Overview** page is now accessed by going to **Status > Overview**.
- The **System configuration** top-level menu option is now just called the **System** menu.
- The HTTPS client certificate validation setting has been moved to the **System administration** page (**System > System**).

Overview and status information

You can view information about the current status, registrations, current calls and call history, and configuration of the Cisco VCS by using the **Status** menu options.

Status overview

The **Overview** page (**Status > Overview**) provides an overview of the current status of the Cisco VCS (or Cisco VCS cluster, if applicable). This page is displayed by default after logging in to the Cisco VCS as an administrator.

The following information is displayed:

Field	Description
System information: many of the items in this section are configurable; click on the item name to be taken to its configuration page.	
System name	The name that has been assigned to the Cisco VCS.
Up time	The amount of time that has elapsed since the system last restarted.
Software version	The version of software that is currently installed on the Cisco VCS.
IPv4 address	The Cisco VCS's IPv4 addresses.
IPv6 address	The Cisco VCS's IPv6 addresses.
Options	The maximum number of calls and registrations, and the availability of additional Cisco VCS features such as TURN Relays, FindMe™, Device Provisioning and Dual Network Interfaces, are controlled through the use of option keys. This section shows all the options that are currently installed on the Cisco VCS.
Resource usage: this shows summary information about the Cisco VCS's resources. If the Cisco VCS is part of a cluster, then details for each peer are shown as well as totals for the entire cluster. To view details of current calls, registrations or TURN relays (Cisco VCS Expressway only), click on the relevant item in the section.	
Non-traversal call licenses	**Current**: the number of non-traversal calls going through the Cisco VCS at this moment. **Peak**: the highest number of concurrent non-traversal calls handled by the Cisco VCS since it was last restarted. **Since last restart**: the total number of non-traversal calls handled by the Cisco VCS since it was last restarted. **License limit**: the number of non-traversal call licenses available on the Cisco VCS.

Field	Description
Traversal call licenses	**Current**: the number of traversal calls going through the Cisco VCS at this moment. **Peak**: the highest number of concurrent traversal calls handled by the Cisco VCS since it was last restarted. **Since last restart**: the total number of traversal calls handled by the Cisco VCS since it was last restarted. **License limit**: the number of traversal call licenses available on the Cisco VCS. See What are traversal calls? for details on what constitutes a traversal call.
Registration licenses	**Current**: the number of aliases registered to the Cisco VCS at this moment. **Peak**: the highest number of aliases concurrently registered to the Cisco VCS since it was last restarted. **Since last restart**: the total number of registrations to the Cisco VCS since it was last restarted. **License limit**: the number of registration licenses available on the Cisco VCS.
TURN relay licenses (Cisco VCS Expressway only)	**Current**: the number of active TURN relays at this moment. **Peak**: the highest number of concurrently active TURN relays since the Cisco VCS was last restarted. **Since last restart**: the total number of TURN relays allocated on the Cisco VCS since it was last restarted. **License limit**: the total number of TURN relay licenses available on the Cisco VCS.

System information

The **System information** page (**Status > System > Information**) provides details of the software, hardware, and time settings of the Cisco 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 Cisco VCS.
Product	This identifies the Cisco VCS.

Field	Description
Software version	The version of software that is currently installed on the Cisco 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 Cisco VCS features such as FindMe™, Device Provisioning and Dual Network Interfaces, are controlled through the use of option keys. This section shows all the optional features currently installed on the Cisco VCS.
Hardware version	The version number of the hardware on which the Cisco VCS software is installed.
Hardware serial number	The serial number of the hardware on which the Cisco VCS software is installed.
Time information section:	
Up time	The amount of time that has elapsed since the system last restarted.
System time (UTC)	The time as determined by the NTP server. If no NTP server has been configured, this will show *Time Not Set*.
Time zone	The time zone that has been configured on the **Time** page.
Local time	If an NTP server has been configured, the system time in local time (UTC adjusted according to the local time zone) is shown. If no NTP server has been configured, the time according to the Cisco VCS's operating system is shown.

Ethernet status

The **Ethernet** page (**Status > System > Ethernet**) shows the MAC address and Ethernet speed of the Cisco VCS.

The page displays the following information for the LAN 1 port and, if the Dual Network Interfaces option key has been installed, the LAN 2 port:

Field	Description
MAC address	The MAC address of the Cisco VCS's Ethernet device for that LAN port.

Field	Description
Speed	The speed of the connection between the LAN port on the Cisco 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 Cisco VCS.

The following information is displayed:

Field	Description
IP section:	
Protocol	Indicates the IP protocol supported by the Cisco VCS. *IPv4*: it only accepts registrations from endpoints using an IPv4 address, and will only take calls between two endpoints or devices communicating via IPv4. It will communicate with other systems via IPv4 only. *IPv6*: it only accepts registrations from endpoints using an IPv6 address, and will only take calls between two endpoints communicating via IPv6. It will communicate 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 Cisco VCS will act as an IPv4 to IPv6 gateway (note that this will require a traversal call license). The Cisco VCS can communicate with other systems via either protocol.
IPv4 gateway	The IPv4 gateway used by Cisco VCS.
IPv6 gateway	The IPv6 gateway used by Cisco VCS.
Dual Network Interfaces	Indicates whether the second LAN port has been enabled. This is done by installing the Dual Network Interfaces option key.
LAN 1	Shows the IPv4 address and subnet mask, and IPv6 address of the LAN 1 port.
LAN 2	If the Dual Network Interfaces 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.

The **Dual network interfaces** option is enabled by the addition of the corresponding option key.

Resource usage

The **Resource usage** page (**Status > System > Resource usage**) provides statistics about the numbers of current and cumulative calls and registrations on the Cisco VCS.

If the Cisco VCS is part of a cluster, then details for each peer are shown as well as totals for the entire cluster.

- **Current**: the number of calls or registrations on the Cisco VCS at this particular moment.
- **Peak**: the highest number of concurrent calls or registrations handled by the Cisco VCS since it was last restarted.
- **Since last restart**: the total number of calls or registrations handled by the Cisco VCS since it was last restarted.
- **License limit**: the total number of licenses available on the Cisco VCS.

To view details of current calls or registrations, click on the relevant item in the section. Note that if your system is a Cisco VCS Expressway, TURN relay license information is also displayed.

This page refreshes automatically every 5 seconds.

Registration status

Registrations by device

The **Registrations by device** page (**Status > Registrations > By device**) lists each device currently registered with the Cisco VCS, and allows you to remove a device's registration. If the Cisco 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 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.
E164	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.
Type	Indicates the nature of the registration. This will most commonly be Endpoint, MCU, Gateway, or SIP UA.
Protocol	Indicates whether the registration is for a SIP 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*.

Field	Description
Address	For H.323 devices this is its RAS address, and for SIP UAs it is the Contact address presented in the REGISTER request.
Peer	Identifies the cluster peer to which the device is registered.

Clicking on a device's **Name** or **E164** number takes you to the Registrations details page for that device.

For a list of all aliases currently registered with the Cisco VCS, see the Registrations by alias page.

Unregistering a device

Click **Unregister** to remove the selected registrations.

Note that:

- if your Cisco 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
- removing a registration does not prevent the same device from automatically re-registering

Filtering the list

To limit the list of registrations, enter one or more characters in the **Filter** field and click **Filter**. Only those registrations that contain (in any of the displayed fields) the string you entered will be shown.

To return to the full list of registrations, click **Reset**.

Registrations by alias

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 Cisco VCS. If the Cisco VCS is part of a cluster, all registrations across the cluster are shown.

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 following information is displayed:

Field	Description
Alias	The H.323 alias, E.164 number, prefix or SIP AOR registered by a device. Clicking on any **Alias** will take you to the Registrations details page for the device that registered that alias.
Alias type	Shows whether the alias is an H.323 ID, E.164 number, prefix or SIP AOR.
Device type	Indicates the nature of the device that registered the alias. This will most commonly be Endpoint, MCU, Gateway or SIP UA.
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 the RAS address. For SIP UAs it is the Contact address presented in the REGISTER request.

Field	Description
Peer	Identifies the cluster peer to which the alias is registered.

Clicking on any **Alias** takes you to the Registrations details page for the device that registered that alias.

For a list of all devices registered with the Cisco VCS, see the Registrations by device page.

Filtering the list

To limit the list of registrations, enter one or more characters in the **Filter** field and click **Filter**. Only those registrations that contain (in any of the displayed fields) the string you entered will be shown.

To return to the full list of registrations, click **Reset**.

Registration history

The **Registration history** page (**Status > Registrations > History**) lists all the registrations that are no longer current. It contains all historical registrations since the Cisco VCS was last restarted. If the Cisco VCS is part of a cluster, the history of all registrations across the cluster is shown.

The following information is displayed:

Field	Description
Name	The H.323 alias or SIP AOR that the device registered. Clicking on an individual **Name** takes you to the Registrations details page for that registration.
E164	For H.323 devices that 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.
Type	Indicates the nature of the registration. This will most commonly be Endpoint, Gateway, or SIP UA.
Protocol	Indicates whether the registration was 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*.
End time	The date and time at which the registration was terminated.
Duration	The length of time that the registration was in place.
Peer	Identifies the cluster peer to which the alias was registered.
Reason	The reason why the registration was terminated.

Filtering the list

To limit the list of registrations, enter one or more characters in the **Filter** field and click **Filter**. Only those registrations that contain (in any of the displayed fields) the string you entered will be shown.

To return to the full list of registrations, click **Reset**.

Registration details

The **Registration details** page (**Status > Registrations > By device**, **Status > Registrations > By alias** or **Status > Registrations > History**, then click on the registration name) shows the particulars of a single registration. The exact details shown here depend on the device's protocol, and whether the registration is still current.

Unregistering and blocking 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** has been set to *Deny List*.)

Call status

Call status

The **Call status** page (**Status > Calls > Calls**) lists all the calls currently taking place to or from devices registered with the Cisco VCS, or that are passing through the Cisco VCS. If the Cisco VCS is part of a cluster, all calls taking place through any Cisco VCS in the cluster are shown.

The following information is displayed:

Field	**Description**
Start time	The date and time when the call was placed.
Source	The alias of the device that placed the call.
Destination	The alias dialed from the device. This may be different from the alias to which the call was placed, which may have been transformed (due to pre-search transforms, zone transforms or User Policy).
Bandwidth allocated	Shows the amount of bandwidth assigned to the call by the Cisco VCS. This may be different to the amount of bandwidth originally requested by the endpoint that placed the call.
Route	The subzone or zone from which the call was received and the subzone or zone to which the call was placed. To see the complete route taken by the call within the Cisco VCS, including intermediary subzones, click **View**.
Protocol	Shows whether the call used H.323, SIP, or both protocols.
Peer	Identifies the cluster peer through which the call is being made.
Actions	Click **View** to go to the Call summary page, which lists further details of this call.

Disconnecting calls

Click **Disconnect** to disconnect the selected calls. Note that if your Cisco 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 Cisco 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 Cisco 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.

Filtering the list

To limit the list of calls, enter one or more characters in the **Filter** field and click **Filter**. Only those calls that contain (in any of the displayed fields) the characters you entered are shown.

To return to the full list of calls, click **Reset**.

Call history

The **Call history** page (**Status > Calls > History**) lists all the calls that are no longer active that have taken place since the Cisco VCS was last restarted. If the Cisco VCS is part of a cluster, all calls that have taken place through any Cisco VCS in the cluster are shown.

The following information is displayed:

Field	Description
Start time	The date and time at which the call was placed.
Source	The alias of the device that placed the call.
Destination	The alias dialed from the device. This may be different from the alias to which the call was placed, which may have been transformed (due to pre-search transforms, zone transforms or User Policy).
Protocol	Shows whether the call used H.323, SIP, or both protocols.
Duration	Shows the length of time of the call.
Status	Shows the reason the call was terminated.
Peer	Identifies the cluster peer through which the call was made.
Actions	Allows you to click **View** to go to the Call summary page, which lists overview details of this call.

Filtering the list

To limit the list of calls, enter one or more characters in the **Filter** field and click **Filter**. Only those calls that contain (in any of the displayed fields) the characters you entered are shown.

To return to the full list of calls, click **Reset**.

Call summary

The **Call summary** page (**Status > Calls > Calls** or **Status > Calls > History**, then click **View** for a particular call) provides overview information about a particular call, including information about the most relevant legs.

Further detailed information about the call can be viewed via the links in the **Related tasks** section at the bottom of the page:

- **View media statistics for this call** takes you to the Call media page, where you can view information about the most relevant session for a call. For traversal calls (i.e. where the Cisco VCS took the media), it will also list the individual media channels (audio, video, data, etc) that made up the call.
- **View all details of this call** takes you to the Call details page, where you can view full information about this call.
- **View search details for this call** takes you to the Search details page, which lists full information about all the searches associated with this call's Call Tag, including the subzones and zones that were searched and any transforms that were applied to the alias being searched for.
- **View all events associated with this call** takes you to the Event Log page, filtered to show only those events associated with this call's Call Tag.

Call details

The **Call details** page lists full information about a particular call, including any failed sessions. This page is reached via the **View all details of this call** link in the **Related tasks** section of either of the following pages:

- the **Call summary** page (**Status > Calls > Calls** or **Status > Calls > History**, then click **View**)
- the **Call details** page (**Status > Calls > Calls** or **Status > Calls > History**, then click **View** for a particular call)

Call media details

The **Call media** page shows information about the most relevant session for a call. For traversal calls (where the Cisco VCS took the media), it also lists the individual media channels (audio, video, data and so on) that made up the call.

This page is reached via the **View media statistics for this call** link in the **Related tasks** section of either of the following pages:

- the **Call summary** page (**Status > Calls > Calls** or **Status > Calls > History**, then click **View**)
- the **Call details** page (**Status > Calls > Calls** or **Status > Calls > History**, then click **View** for a particular call)

Search history

The **Search history** page (**Status > Search history**) lists the most recent 255 searches that have taken place since the Cisco VCS was last restarted.

About searches

Before a call can be placed, the endpoint being called must be located. The Cisco 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).

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 calls, enter one or more characters in the **Filter** field and click **Filter**. Only those calls that contain (in any of the displayed fields) the characters you entered will be shown.

To return to the full list of calls, click **Reset**.

Viewing associated searches

If there were other searches associated with the same call, a **View all searches associated with this call tag** link is shown at the bottom of the page; clicking this takes you to a Search details page showing all searches relating to that particular call.

Search details

The **Search details** page (**Status > Search history**, then click **View** for a particular search) lists full information about either an individual search, or all searches associated with a single call (depending on how you reached the page). The information shown includes:

- the subzones and zones that were searched
- the call path and hops
- any transforms that were applied to the alias being searched for
- use of policies such as Admin Policy 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 summary 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 Cisco VCS that together make up the Local Zone. This will always include 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 Cisco 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 Cisco VCS, the number of calls and amount of bandwidth being used by each, and their current status.

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 Cisco VCS. Clicking on a zone **Name** takes you to the configuration page for that subzone.
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.
Status	The current status of each zone.

Link status

The **Link status** page (**Status > Bandwidth > Links**) lists all of the links currently configured on the Cisco 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 Cisco 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 service status

The **Policy service status** page (**Status > Policy services**) lists all of the policy services configured on the Cisco VCS and displays their current status.

The set of policy services includes all of the services defined on the **Policy services** page (**VCS 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.

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 Cisco VCS.
Status	The current status of the service.
Last used	Indicates when the service was last requested by a Cisco VCS process.

TURN relays status

The **TURN relays** page (**Status > TURN relays**) lists all the currently active TURN Relays on the Cisco VCS. For each relay, it shows the requesting client address and port and the corresponding Cisco VCS address and port.

Note: TURN services are available on Cisco VCS Expressways only. They are configured from the **TURN** page (**VCS configuration > Expressway > TURN**).

The following information is displayed:

Field	Description
Relay	The index number of the relay.
Address	The IP address and port on the Cisco VCS of the relay resource that has been allocated for this particular request.
Client	The IP address and port on the NAT (or the client if there is no NAT) that requested the relay.
Creation time	The date and time the relay became active.
Expiry time	The date and time the relay will become inactive.

Viewing TURN relay details

Click **View** to go to the TURN relay summary page where you can see more information about a relay. From here further detailed information about the relay can be viewed by using the links in the **Related tasks** section at the bottom of the page:

- **View permissions for this relay** takes you to the **TURN relay permissions** page, where you can view information about the permissions that have been defined on the relay.
- **View channels for this relay** takes you to the **TURN relay channels** page, where you can view information about the channel bindings that have been defined on the relay.
- **View counters for this relay** takes you to the **TURN relay counters** page, where you can view TURN request, response and error counters, as well as media counters, for the relay.

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 Cisco 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 Cisco 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: FindMe users will not be 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.

OCS Relay status

The **OCS Relay status** page (**Status > Applications > OCS Relay**) lists all the FindMe IDs being handled by the OCS Relay application, and shows the current status of each.

The OCS Relay application is required in deployments that use both Microsoft Office Communicator (MOC) clients and FindMe, if they both use the same SIP domain. Its purpose is to:

- enable the Cisco VCS to share FindMe presence information with MOC clients
- enable the Microsoft Office Communications Server (OCS) to forward calls to FindMe IDs

Note: the OCS Relay application is configured via the OCS Relay page (**Applications > OCS Relay**).

The following information is displayed:

Field	Description
Alias	The FindMe ID being handled by the OCS 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 OCS. Doing so allows OCS to forward calls to the FindMe ID.
Subscription state	Indicates whether the OCS Relay application has subscribed successfully to the FindMe ID's presence information. Doing so allows MOC clients to view the presence information of FindMe users.

Provisioning status

The **Provisioning status** page (**Status > Applications > Provisioning**) shows the status of the Cisco VCS's provisioning server and phone book server.

These servers provide provisioning-related services to provisioned devices, without the need for Cisco TMS.

Provisioning server

The provisioning server provides basic device provisioning to provisioned users.

This section displays the server's status and summarizes the subscription requests received by the server since the Cisco 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

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 since the Cisco VCS was last restarted.

Note that the Cisco VCS's provisioning facilities are only available if the Starter Pack option key is installed.

Warnings

The **Warnings** page (**Status > Warnings**, or by clicking on the red warning icon ⚠ which appears at the top right of any page when a warning is in place) provides a list of all the warnings currently in place on your system (and, in the **Action** column where applicable, their proposed resolution).

You should deal with each warning by clicking each **Action** hyperlink and making the necessary configuration changes to resolve the problem.

Warnings occur when an event or configuration change has taken place on the Cisco VCS that requires some manual administrator intervention such as a restart. Warnings may also be raised for hardware and environmental issues such as faulty disks and fans or high temperatures.

Acknowledging a warning (by selecting a warning and clicking on the **Acknowledge** button) removes the warning icon from the web UI, but the warning will still be listed on the **Warnings** page with a status of *Acknowledged*. If a new warning occurs, the warning icon will reappear.

You cannot delete warnings from the **Warnings** page. Warnings are removed by the Cisco VCS only after the required action or configuration change has been made.

After a restart of the Cisco VCS, any *Acknowledged* warnings that are still in place on the Cisco VCS will reappear with a status of *New*, and must be re-acknowledged.

Refer to the warnings list for further information about the specific warnings that can be raised.

Hardware status

The **Hardware** page (**Status > Hardware**) provides information about the physical status of your Cisco VCS unit.

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.

CAUTION: 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.

Event Log

The **Event Log** page (**Status > Logs > Event Log**) lets you view and search the Event Log, which is a list of all the events that have occurred on your system since the last upgrade. The Event Log holds 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. 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 Event Log listing, click **Reset**.

Reconfiguring the log settings

Clicking **Reconfigure 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.

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
- Installation of <item> succeeded
- Registration Accepted
- Call Connected
- Request Successful
- Beginning System Restore
- Completed System Restore

Orange events:

- System Shutdown

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

For more information about the format and content of the Event Log see Event Log format and Events and levels.

Configuration Log

The **Configuration Log** page (**Status > Logs > Configuration Log**) provides a list of all changes to the Cisco VCS configuration made using the web or command line interface (CLI).

The configuration log visible using the web interface holds a maximum of 4MB of data; when this size is reached, the oldest entries are overwritten.

Filtering the Configuration Log

The **Filter** section lets you filter the Configuration Log. 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 Configuration 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 Cisco 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

Cisco VCS unit front panel

The LCD panel on the front of the Cisco VCS hardware unit has a rotating display of the Cisco VCS's system name, IP addresses, warnings, and the number of current traversal calls, non-traversal calls and registrations.

Network and system settings

This section describes all the options that appear under the **System** menu of the web interface.

These options enable you to configure the Cisco VCS in relation to the network in which it is located, for example its IP settings and the external services used by the Cisco VCS (for example DNS, NTP and SNMP).

Configuring IP settings

The **IP** page (**System > IP**) is used to configure the IP protocols and settings of the Cisco VCS.

IP protocol configuration

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

- *IPv4*: 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*: 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 Cisco VCS acts as an IPv4 to IPv6 gateway. It communicates with other systems via either protocol.

Note: some endpoints support both IPv4 and IPv6, however an endpoint can use only one protocol when registering with the Cisco VCS. Which protocol it uses is determined by the format used to specify the IP address of the Cisco VCS on the endpoint. After the endpoint has registered using either IPv4 or IPv6, the Cisco 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 Cisco VCS.

IPv4 to IPv6 gatewaying (interworking)

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

IP gateways and IP routes (static routes)

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

However, you can also configure additional IP routing information (static routes) on the Cisco VCS. This is sometimes required when using the Dual Network Interfaces option and occasionally required in other complex network deployments. You can configure routes for up to 50 networks and host combinations. IP routes can be configured using the CLI only.

LAN configuration

LAN 1 is the primary network port on the Cisco VCS.

You can configure the **IPv4 address** and **subnet mask**, and **IPv6 address** for this port.

For Cisco VCS Expressway boxes behind a static NAT, you can also configure the NAT's IP address. If you have Dual Network Interfaces installed, you can also configure these options for the LAN 2 port.

The Cisco VCS is shipped with a default IP address of 192.168.0.100 (for both LAN ports). This lets you connect the Cisco VCS to your network and access it via the default address so that you can configure it remotely.

The **External LAN interface** field indicates which LAN port has been connected to your external network. It also determines the port from which TURN server relay allocations are made.

About Dual Network Interfaces

The Dual Network Interface option key enables the LAN 2 port on the Cisco VCS Expressway for both management and call signaling. This allows you to have a second IP address for your Cisco VCS.

This configuration is intended for high-security deployments where the Cisco VCS 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 Cisco VCS.

To enable this feature you must purchase and install the appropriate option key. Contact your Cisco representative for information.

Note: you should configure the LAN 1 port and restart the Cisco VCS before configuring the LAN 2 port.
If you have Dual Network Interfaces enabled but only want to configure one of the Ethernet ports, you must use LAN 1.

About static NAT

It is possible to deploy a Cisco 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 Cisco VCS Expressway is located in a DMZ, and has the **Dual Network Interfaces** feature enabled.

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

In such a deployment, when configuring traversal clients to use the Cisco VCS Expressway as a traversal server, it is the latter internally-facing IP address of the Cisco VCS Expressway that should be used. To enable the use of a static NAT:

1. Ensure that the Dual Network Interfaces option key is installed.
2. For the externally-facing LAN port:
   a. In the **IPv4 address field**, enter the Cisco VCS Expressway's private IP address.
   b. Select an **IPv4 static NAT mode** of *On*.
   c. In the **IPv4 static NAT address** field, enter the Cisco VCS Expressway's public IP address - this is the IP address of the outside of the NAT.

Configuring Ethernet settings

The **Ethernet** page (**System > Ethernet**) is used to configure the speed of the connection between the Cisco VCS and the Ethernet switch to which it is connected. The speed must be set to the same value on both systems. If you have the **Dual network interfaces** option enabled, you can configure the Ethernet speed separately for each LAN port.

The default is *Auto*, which means that the two systems will auto-negotiate the appropriate speed.

Note: you are recommended to use the default value of **Auto** unless the switch to which you are connecting is unable to auto-negotiate. A mismatch in Ethernet speed settings between the Cisco VCS and Ethernet switch will at best result in packet loss; at worst it will make the system inaccessible for endpoints and system administrators.

Configuring DNS settings

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

DNS servers

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

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

You can specify up to 5 DNS servers. The Cisco VCS sends requests to all configured servers in parallel, taking the first result received and discounting the rest.

Note: this can lead to confusing behavior should local network administrators, for example, deploy "split horizon" DNS where records held on an internal, corporate, DNS server use the same domain names but with different values to those on the public internet - an often used tactic in corporate intranets.

DNS settings

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

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

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

It applies to the following configuration settings in the Cisco VCS:

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

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

Tip: the FQDN of the Cisco VCS is the **Local host name** plus the **Domain name**.

Impact on SIP messaging

The **Local host name** and **Domain name** are also used to identify references to this Cisco VCS in SIP messaging, where an endpoint has configured the Cisco 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 Cisco VCS may, for example, reject an INVITE request if the FQDN configured on the endpoint does not match the **Local host name** and **Domain name** configured on the Cisco 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 Cisco VCS.)

Configuring Quality of Service settings

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

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

Supported mechanisms

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

Configuring system name and access settings

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

Configuring the system name

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

You are recommended to give the Cisco VCS a name that allows you to easily and uniquely identify it.

Administration access

While it is possible to administer the Cisco VCS via a PC connected directly to the unit via a serial cable, you may want to access the system remotely over IP. You can do this using either or both:

- the web interface, via HTTPS
- a command line interface, via SSH or Telnet

The configurable options are:

Field	Description	Usage tips
Session time out	The number of minutes that an administration session (serial port, HTTPS, Telnet or SSH) may be inactive before the session is timed out. Default is 0.	A value of 0 means that session time outs are disabled.
Telnet service	Determines whether the Cisco VCS can be accessed via Telnet. Default is **Off**.	
SSH service	Determines whether the Cisco VCS can be accessed via SSH and SCP. Default is **On**.	

Field	Description	Usage tips
Web interface (over HTTPS)	Determines whether the Cisco VCS can be accessed via the web interface. Default is **On**.	Cisco TMS accesses the Cisco VCS via the web server. If HTTPS mode is turned off, Cisco TMS will not be able to access it.
Client certificate validation	Controls whether client systems (typically web browsers) that communicate with the Cisco VCS over HTTPS have to present a valid client certificate before the connection can be established. Default is **Off**.	Enabling this feature means that your browser can use the Cisco VCS web interface only if it has a valid client certificate signed by a CA in the Cisco VCS's trusted CA certificate list. Ensure your browser (the client system) has a valid (in date and not revoked if using a CRL) 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 trusted CA certificates, manage client certificate revocation lists and test client certificates on the security certificates page. Note that this feature does not affect client verification of the Cisco VCS's server certificate.
Redirect HTTP requests to HTTPS	Determines whether HTTP requests are redirected to the HTTPS port. Default is **On**.	HTTPS must also be enabled for access via HTTP to function.

Note: by default, access via HTTPS and SSH is enabled; access via Telnet is disabled. To securely manage the Cisco VCS you should disable Telnet, using the encrypted HTTPS and SSH protocols instead. For further security, disable HTTPS and SSH as well and use the serial port to manage the system.

Because access to the serial port allows the password to be reset, it is recommended that you install the Cisco VCS in a physically secure environment.

Cisco VCS unit front panel

The LCD panel on the front of the Cisco VCS hardware unit has a rotating display of the Cisco VCS's system name, IP addresses, warnings, and the number of current traversal calls, non-traversal calls and registrations.

You can configure the front panel to hide this identifying information, if required for security reasons for example, by using the CLI command **xConfiguration Administration LCDPanel Mode**. If the mode is set to *Off* the front panel only displays "Cisco".

Configuring SNMP settings

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

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

The Cisco VCS supports the most basic MIB-II tree (.1.3.6.1.2.1) as defined in *RFC 1213* [23].

The information made available by the Cisco VCS includes the following:

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

By default, SNMP is *Disabled*, therefore to allow the Cisco 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. *SNMPv3 (secure SNMP)*: supports authentication and encryption. *SNMPv3 plus TMS support*: secure SNMPv3 plus non-secure access to OID 1.3.6.1.2.1.1.2.0 only. *SNMPv2c*: 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 *SNMPv3 plus TMS support*.
Community name	The Cisco VCS's SNMP community name. The default is *public*.	Only applies to *SNMPv2c* and *SNMPv3 plus TMS support*.
System contact	The name of the person who can be contacted regarding issues with the Cisco VCS.	The **System contact** and **Location** are used for reference purposes by administrators when following up on queries.
Location	Specifies the physical location of the Cisco VCS.	
Username	The Cisco VCS's SNMP username, used to identify this SNMP agent to the SNMP manager.	Only applies when using secure SNMPv3.
Authentication settings (only applicable to SNMPv3)		
Authentication mode	Enables or disables SNMPv3 authentication.	

Field	Description	Usage tips
Type	The algorithm used to encrypt authentication credentials. *SHA*: Secure Hash Algorithm. *MD5*: Message-Digest algorithm 5.	
Password	The password used to encrypt authentication credentials.	Must be at least 8 characters.
Privacy settings (only applicable to SNMPv3)		
Privacy mode	Enables or disables SNMPv3 encryption.	
Type	The security model used to encrypt messages. *DES*: Data Encryption Standard 56-bit encryption. *AES*: Advanced Encryption Standard 128-bit encryption.	
Password	The password used to encrypt messages.	Must be at least 8 characters.

The Cisco 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 Cisco VCS on the public internet or in any other environment where you do not want to expose internal system information.

Configuring time zone and NTP server settings

The **Time** page (**System > Time**) is used to configure the Cisco VCS's NTP server and specify your local time zone.

NTP server

The NTP server is a remote server with which the Cisco VCS synchronizes in order to ensure its time setting is accurate. The NTP server provides the Cisco VCS with UTC time. Accurate timestamps play an important part in H.323 authentication, helping to guard against replay attacks. For this reason, if you are using authentication in a deployment that includes H.323, both the Cisco VCS and the endpoints must use an NTP server to synchronize their system time.

Accurate time is also necessary for configuration replication to work properly if the Cisco VCS is in a cluster, and to ensure correct timestamps in system logs.

Traversal clients must always authenticate with traversal servers (even if the traversal server is not using device authentication for endpoint clients). Therefore, for a traversal client and traversal server to connect to each other, both must be configured with details of an NTP server.

SIP-only deployments do not require the use of NTP for authentication.

To configure the Cisco VCS with an **NTP server**, enter the IP address or FQDN (or server address, if a DNS **Domain name** has also been configured) of the NTP server to be used when synchronizing system time.

- The **NTP server** field defaults to one of four NTP servers provided by Cisco, either: *0.ntp.tandberg.com*, *1.ntp.tandberg.com*, *2.ntp.tandberg.com* or *3.ntp.tandberg.com*.
- The connection status to the NTP server is shown in the **Status** section.

Cisco VCS time display and time zones

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 and Configuration Log.

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

Specifying your local **Time zone** lets the Cisco VCS determine the local time where the system is located. It does this by offsetting UTC time by the number 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).

The **Time** page displays both UTC and local time in the **Status** section. Note that a UTC system timestamp is included at the end of each entry in the Event Log and Configuration Log.

Configuring the Login page

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

The **Welcome message title** and **text** will appear to administrators when attempting to log in using the CLI, and to FindMe users and administrators when attempting to log in using the web interface.

You can upload an image that will appear on the login page, above the welcome message, to FindMe users and administrators when attempting to log in using the web interface.

- supported image file formats are JPG, GIF and PNG
- images larger than 200x200 pixels will be scaled down

Note that this feature is not configurable using the CLI.

Configuring external manager settings

The **External manager** page (**System > External manager**) allows you to configure the Cisco VCS's external manager settings.

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

Field	Description	Usage tips
Address and **path**	To use an external manager, you must configure the Cisco 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**.

Field	Description	Usage tips
Protocol	Determines whether communications with the external manager are over **HTTP** or **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 Cisco VCS's trusted CA certificates. This is done from the Security certificates page (**Maintenance > Security certificates**).

Configuring logging levels

The Cisco VCS provides an event logging facility for troubleshooting and auditing purposes. The Event Log records information about such things as calls, registrations, and messages sent and received.

The **Logging** page (**System > Logging**) lets you:

- Specify the **Log level** to set the amount of information to record.
- Copy the event log to a **remote syslog server**.

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
Level 1	High-level events such as registration requests and call attempts. Easily human readable. For example: ▪ call attempt/connected/disconnected ▪ registration attempt/accepted/rejected
Level 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
Level 3	All Level 1 and Level 2 Events, plus: ▪ protocol keepalives ▪ call-related SIP signaling messages
Level 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 Cisco VCS, and the level at which they are logged.

You can control which events are logged by the Cisco VCS by setting the **Log level**. All events with a level numerically equal to and lower than the specified logging level are recorded in the Event Log. So, at level 1, only level 1 events are logged; at level 2, both level 1 and level 2 events are logged, and so on. The default log level is *1*.

Note that:

- Logging at level 3 or level 4 is not usually recommended as the Event Log holds a maximum of 2GB of data and logging at these levels on a busy system could cause the Event Log to be recycled too quickly.
- Changes to the event log level affect both the Event Log that you can view via the web interface, and the information that is copied to the remote log server (if any) that you have configured.
- Changes to the event log level are not retrospective. If you change the event log level, it will only effect what is logged from that point onwards.

Remote logging

The Event Log is always stored locally on the Cisco VCS. However, it is often convenient to collect copies of all event logs from various systems in a single location. A computer running a BSD-style syslog server, as defined in *RFC 3164* [4], may be used as the central log server. Note that:

- A Cisco VCS will not act as a central logging server for other systems.
- Events are always logged locally (to the Event Log) regardless of whether or not remote logging is enabled.
- The Cisco VCS may use any of the 23 available syslog facilities for different messages. Specifically, LOCAL0..LOCAL7 (facilities 16..23) are used by different components of the application software on the Cisco VCS.

To enable remote logging, you must configure the Cisco VCS with the IP addresses or Fully Qualified Domain Names (FQDNs) of the **Remote syslog servers** to where the Event Log is written. Up to 4 servers can be specified. Note that these servers cannot be another Cisco VCS.

Protocols

This section provides information about the pages that appear under the **VCS configuration > Protocols** menu.

It includes the following information:

- an overview of H.323 and the H.323 configuration options available on the Cisco VCS
- an overview of SIP and the SIP configuration options available on the Cisco VCS
- how to configure the Cisco VCS to act as a SIP to H.323 gateway

About H.323

The Cisco VCS supports the H.323 protocol: it is an H.323 gatekeeper.

It will also provide interworking between H.323 and SIP, translating between the two protocols to enable endpoints that only support one of these protocols to call each other. In order to support H.323, the **H.323 mode** must be enabled.

Using the Cisco VCS as an H.323 gatekeeper

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

To enable the Cisco VCS as an H.323 Gatekeeper, you must ensure that **H.323 mode** is set to *On* (**VCS configuration > Protocols > H.323**).

Note that this is the default setting, so the Cisco VCS will work as an H.323 gatekeeper "out of the box", without any other special configuration.

H.323 endpoint registration

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

There are two ways an H.323 endpoint can locate a Cisco 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 Cisco VCS it can find. It does this by sending out a Gatekeeper Discovery Request, to which eligible Cisco VCSs will respond.
- If the mode is set to manual, you must specify the IP address of the Cisco VCS with which you want your endpoint to register, and the endpoint will attempt to register with that Cisco VCS only.

Preventing automatic H.323 registrations

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

About SIP

The Cisco VCS supports the SIP protocol. It acts as a SIP registrar, SIP proxy and as a SIP Presence Server.

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

To support SIP:

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

Cisco 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. When a call is received for that AOR, the SIP registrar refers to the record in order to find the endpoint to which it corresponds. (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 Cisco VCS or Cisco VCS cluster.)

A SIP registrar only accepts registrations for domains for which it is authoritative. The Cisco VCS can act as a SIP registrar for up to 20 domains.

SIP aliases always take the form **username@domain**. To make the Cisco 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 with an alias that includes that domain.

Whether or not the Cisco VCS accepts a registration request depends on its registration control settings.

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 (Cisco VCS or Cisco VCS cluster) with which they want to register, and the endpoint will attempt to register with that registrar only.

The Cisco VCS is a SIP server and a SIP registrar.

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

SIP registration resiliency

The Cisco VCS supports multiple client-initiated connections (also referred to as "SIP outbound") as outlined in *RFC 5626* [41].

This allows SIP endpoints that support *RFC 5626* to be simultaneously registered to multiple Cisco 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.

Cisco VCS as a SIP proxy server

The Cisco 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 Cisco 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 Cisco 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 a Cisco VCS, the Cisco VCS adds a path header component to the request. This signals that calls to that endpoint should be routed through the Cisco VCS. This is usually required in situations where firewalls exist and the signalling must follow a specified path to successfully traverse the firewall. For more information about path headers, see *RFC 3327* [10].

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

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

Accepting proxied registration requests

If the Cisco VCS receives a proxied registration request, in addition to the Cisco VCS's standard registration controls, you can also control whether the Cisco 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 Cisco VCS.

Cisco VCS as a SIP Presence Server

The Cisco 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 full information on how to enable and use the Cisco VCS as a SIP Presence server, see the Presence section.

Movi v2.0 (or later) clients

As for any other SIP endpoint, the Cisco VCS acts as a SIP registrar and SIP proxy for Movi™ v2.0 (or later) clients - no other special support or configuration is required on the Cisco VCS.

H.323 configuration

The **H.323** page (**VCS configuration > Protocols > H.323**) is used to enable and disable H.323 on the Cisco VCS, and configure H.323-specific ports and settings.

Field	Description	Usage tips
H.323 mode	Enables or disables H.323 on the Cisco VCS. H.323 support is *On* by default	
Registration UDP port	The listening port for H.323 UDP registrations. Default is 1719.	The default Cisco VCS configuration uses standard port numbers so you can use H.323 services out of the box without having to first set these up.
Call signaling TCP port	The listening port for H.323 call signaling. Default is 1720.	
Call signaling port range start and **end**	Specifies the lower port in the range used by H.323 calls after they are established. Default is 15000.	The call signaling port range must be great enough to support all the required concurrent calls.
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 Cisco VCS using an alias that has already been registered on the Cisco 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.

Field	Description	Usage tips
Time to live	The interval (in seconds) at which an H.323 endpoint must re-register with the Cisco 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.
Call time to live	The interval (in seconds) at which the Cisco 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 will be disconnected. The system polls endpoints in a call regardless of 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 Cisco VCS, set **Auto discover** to *Off*. This means that endpoints can only register with the Cisco VCS if their **Gatekeeper Discovery** setting is *Manual* and they have been configured with the Cisco 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.

SIP configuration

The **SIP** page (**VCS configuration > Protocols > SIP > Configuration**) is used to enable and disable SIP on the Cisco VCS, and configure SIP-specific ports and settings.

Field	Description	Usage tips
SIP mode	Enables and disables SIP functionality (SIP registrar and SIP proxy services) on the Cisco VCS. Default is *On*.	This mode must be enabled to use either the Presence Server or the Presence User Agent.
Registration expire delta (seconds)	The period within which a SIP endpoint must re-register with the Cisco VCS to prevent its registration expiring. Default is 60.	This applies only to endpoints registered with the Cisco VCS. It does not apply to endpoints whose registrations are proxied through the Cisco VCS.

Field	Description	Usage tips
SIP registration proxy mode	Specifies how proxied registrations and requests containing Route Sets are handled. *Off*: registration requests are not proxied (but are still permitted locally if the Cisco VCS is authoritative 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. Default is *Off*.	
SIP protocols and ports	The Cisco VCS supports SIP over **UDP**, **TCP** and **TLS** transport protocols. You can configure whether or not incoming and outgoing connections using each protocol are supported, and if so, the ports on which the Cisco VCS listens for such connections. This is done using the **Mode** and **Port** settings for each protocol. The default mode for each protocol is *On*; the default ports are: ▪ UDP port: 5060 ▪ TCP port: 5060 ▪ TLS port: 5061	At least one of the transport protocols must be set to a **Mode** of *On* for SIP functionality to be supported.
TCP outbound port start / end	The range of ports the Cisco VCS uses when TCP and TLS connections are established. The default range is 25000 to 29999.	The range must be sufficient to support all required concurrent connections.
Session refresh interval (seconds)	The maximum time allowed between session refresh requests for SIP calls. Default is 1800.	For further information refer to the definition of *Session-Expires* in *RFC 4028* [14].
Minimum session refresh interval (seconds)	The minimum value the Cisco VCS will negotiate for the session refresh interval for SIP calls. Default is 500.	For further information refer to the definition of *Min-SE header* in *RFC 4028* [14].

Field	Description	Usage tips
Require UDP BFCP mode	Controls whether the Cisco VCS requires the use of the **com.tandberg.udp.bfcp** extension for endpoints that support it.	The default settings for these modes are not supported by some neighbor systems so make sure you select the appropriate zone profile when configuring zones.
Require Duo Video mode	Controls whether the Cisco VCS requires the use of the **com.tandberg.sdp.duo.enable** extension for endpoints that support it.	

Configuring SIP domains

The **Domains** page (**VCS configuration > Protocols > SIP > Domains**) lists the SIP domains for which the Cisco VCS is authoritative. The Cisco VCS will act as a SIP Registrar and Presence Server for these domains, and will accept registration requests for any SIP endpoints attempting to register with an alias that includes these domains.

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**.

Configuring SIP and H.323 interworking

The **Interworking** page (**VCS configuration > Protocols > Interworking**) lets you configure whether or not the Cisco VCS acts as a gateway between SIP and H.323 calls.

The Cisco VCS is able to act as a gateway between SIP and H.323, translating calls from one protocol to the other. This is known as “interworking”.

By default, the Cisco 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 Cisco VCS will act 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 Cisco VCS will not act as a SIP-H.323 gateway.
- *Registered only*: the Cisco VCS will act as a SIP-H.323 gateway but only if at least one of the endpoints is locally registered.
- *On*: the Cisco VCS will act as a SIP-H.323 gateway regardless of whether the endpoints are locally registered.

You are recommended to leave this setting as *Registered only* (where calls are interworked only if at least one of the endpoints is locally registered). 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.

Searching by protocol

When searching a zone, the Cisco VCS will first perform the search using the protocol of the incoming call. If the search was unsuccessful the Cisco VCS may then search the zone again using the alternative protocol, depending on where the search came from and the **Interworking mode**.

- If the request has come from a neighboring system and **Interworking mode** is set to *Registered only*, the Cisco VCS will search 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 Cisco VCS will search the local zone and all external zones using both protocols.

Note: calls for which the Cisco VCS acts as a SIP to H.323 gateway are traversal calls. They will therefore require a traversal call license.

Enabling SIP endpoints to dial H.323 numbers

SIP endpoints can only make calls in the form of URIs - e.g. **name@domain**. If the caller does not specify a domain when placing the call, the SIP endpoint will automatically append 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 Cisco VCS won't 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 Cisco VCS that strips the **@domain** portion of the alias for those URIs that are in the form of **number@domain**.
  Refer to the pre-search transforms section for information about how to configure pre-search transforms, and to the stripping @domain for dialing to H.323 numbers section for an example of how to do this.

Registration control

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

It includes the following information:

- an overview of the Cisco VCS's registration policies
- how to control registrations using Allow Lists and Deny Lists

About registrations

For an endpoint to use the Cisco VCS as its H.323 gatekeeper or SIP registrar, the endpoint must first register with the Cisco VCS. The Cisco 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, the Cisco VCS's on-box directory service or an external policy service to specify which aliases can and cannot register with the Cisco 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 Cisco VCS.

For specific information about how registrations are managed across peers in a cluster, see the Sharing registrations across peers section.

Finding a Cisco VCS with which to register

Before an endpoint can register with a Cisco VCS, it must determine which Cisco 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 Cisco VCS Expressway

If a traversal-enabled endpoint registers directly with a Cisco VCS Expressway, the Cisco VCS Expressway will provide the same services to that endpoint as a Cisco 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 Cisco 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 Cisco VCS. They are known as locally registered services. These systems are configured with their own prefix, which they provide to the Cisco VCS when registering. The Cisco 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.

Note that the Cisco TelePresence MPS 200 and MPS 800, and the Cisco TelePresence Content Server both support Expressway. They can therefore register directly with a Cisco VCS Expressway for firewall traversal.

Configuring registration restriction policy

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

The **Restriction policy** option specifies the policy to use when determining which endpoints may register with the Cisco 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.
- *Directory*: only endpoints that register an alias listed in the directory service may register.
- *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.

Policy service

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:

Field	Description	Usage tips
Protocol	The protocol used to connect to the policy service.	The Cisco VCS automatically supports HTTP to HTTPS redirection when communicating with the policy service server.
Certificate verification mode	Controls whether the certificate presented by the policy service is verified when connecting over HTTPS.	When enabled, the value specified in the **Server address** field must be contained within the server's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes).

Field	Description	Usage tips
HTTPS certificate revocation list (CRL) checking	Controls certificate revocation list checking of the certificate supplied by the policy service. When enabled, the server's X.509 certificate is checked against the HTTPS certificate revocation list.	CRL data is uploaded to the Cisco VCS via the **HTTPS certificate revocation list** file on the Security certificates page.
Server address 1 - 3	The IP address or Fully Qualified Domain Name (FQDN) of the service.	For resiliency, up to three server addresses can be supplied.
Path	The URL of the service.	
Username	The username used by the Cisco VCS to log in and query the service.	
Password	The password used by the Cisco VCS to log in and query the service. The maximum plaintext length is 30 characters (which is subsequently encrypted).	
Default CPL	The default CPL used by the Cisco VCS if the policy service is unavailable.	This defaults to **<reject status='403' reason='Service Unavailable'/>** but you could change it, for example, to redirect to an answer service or recorded message.

Registering aliases

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

H.323

When registering, the H.323 endpoint presents the Cisco 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 Cisco 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.

Attempts to register using an existing alias

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

- **H.323**: an H.323 endpoint may attempt to register with the Cisco VCS using an alias that has already been registered on the Cisco VCS from another IP address. You can control how the Cisco VCS behaves in this situation by configuring the **Registration conflict mode**, on the H.323 page (**VCS 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 Cisco 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 Cisco 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 expire delta** setting for SIP (**VCS configuration > Protocols > SIP > Configuration**) and the **Time to live** setting for H.323 (**VCS configuration > Protocols > H.323**).

About Allow and Deny Lists

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

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

For example, if the **Restriction policy** is set to *Deny List* and an endpoint attempts to register using three aliases, one of which matches a pattern on the Deny List, that endpoint's registration will be denied. Likewise, if the **Restriction policy** is set to *Allow List*, only one of the endpoint's aliases needs to match a pattern on the Allow List for it to be allowed to register using all its aliases.

Allow Lists and Deny Lists are mutually exclusive: only one may be in use at any given time. You can also control registrations at the 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 (**VCS configuration > Registration > Allow List**) shows the endpoint aliases and alias patterns that are allowed to register with the Cisco 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
Pattern	The pattern against which an alias is compared.	
Type	The way in which the **Pattern** must match the alias. Options are: *Exact*: the alias must match the **Pattern** exactly. *Prefix*: the alias must begin with the **Pattern**. *Suffix*: the alias must end with the **Pattern**. *Regex*: the **Pattern** is a regular expression.	You can test whether a pattern matches a particular alias by using the **Check pattern** tool (**Maintenance > Tools > Check pattern**).
Description	An optional free-form description of the entry.	

Configuring the registration Deny List

The **Registration Deny List** page (**VCS configuration > Registration > Deny List**) shows the endpoint aliases and alias patterns that are **not** allowed to register with the Cisco 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
Pattern	The pattern against which an alias is compared.	
Type	The way in which the **Pattern** must match the alias. Options are: *Exact*: the alias must match the **Pattern** exactly. *Prefix*: the alias must begin with the **Pattern**. *Suffix*: the alias must end with the **Pattern**. *Regex*: the **Pattern** is a regular expression.	You can test whether a pattern matches a particular alias by using the **Check pattern** tool (**Maintenance > Tools > Check pattern**).
Description	An optional free-form description of the entry.	

Device authentication

This section provides information about the Cisco VCS's Authentication Policy and the pages that appear under the **VCS configuration > Authentication** menu.

It includes the following information:

- an overview of device authentication and how to configure the Cisco VCS's Authentication Policy
- how to configure the Cisco VCS to authenticate endpoints against either the Cisco VCS's local database or a remote LDAP database
- how to configure the username and password that is used by the Cisco VCS whenever it is required to authenticate with external systems

About device authentication

Device authentication controls whether systems attempting to communicate with the Cisco VCS must authenticate with it first.

The Cisco VCS can be configured to allow both authenticated and unauthenticated endpoints to register to the same Cisco VCS, but to subsequently control what those endpoints can do based upon their authentication status.

Authentication Policy

The Cisco VCS's Authentication Policy is applied at the zone and subzone levels. It controls how the Cisco VCS authenticates incoming messages from that zone or subzone and whether those messages are rejected or are subsequently treated as authenticated or unauthenticated within the Cisco VCS.

The Authentication Policy settings allow you to:

- **control registrations via subzones**: when authentication is enabled for a particular subzone, endpoints must authenticate with the Cisco VCS before they can register
- **limit the services available to unregistered or unauthenticated endpoints and devices**: search rules and CPL can be restricted to only apply to authenticated requests
- **cater for endpoints from third-party suppliers that do not support authentication within their registration mechanism**: assign registrations requests for particular devices into a subzone that is configured to treat all such trusted endpoints registered within that subzone as authenticated

See Authentication Policy configuration options for a full description of how the policy is applied per zone and subzone, and how its behavior varies depending on message protocol.

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 Cisco VCS depends on the protocol being used:

- **H.323**: any necessary credentials are contained within the incoming request.
- **SIP**: credentials are not contained within the initial request. Instead the Cisco 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 Cisco 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 Cisco VCS chooses to trust any authentication carried out at an earlier stage by configuring a zone's SIP authentication trust setting.

The Cisco VCS can check the credentials supplied within the message against either a local database or a remote LDAP repository. See Device authentication configuration for more information.

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

Authentication Policy configuration options

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

The Cisco VCS's Authentication Policy at the zone level controls how the Cisco VCS authenticates incoming messages from that zone. Note that the Authentication Policy is configurable for the Default Zone but does not apply to DNS and ENUM zones.

To configure a zone's **Authentication policy**, go to the **Edit zone** page (**VCS configuration > Zones**, then click **View/Edit** or the name of the zone). The policy is set to *Do not check credentials* by default.

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

H.323

Authentication 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 Cisco 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 Cisco VCS is authoritative) or a non-local domain.

Authentication 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.

Authentication policy	Trust	In local domain	Outside local domain
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 Cisco 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.
	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

The Cisco VCS's Authentication Policy at the subzone level controls how the Cisco VCS authenticates incoming messages (including registration requests) from that subzone.

To configure a subzone's **Authentication policy**, go to the **Edit subzone** page (**VCS configuration > Local Zone > Subzones**, then click **View/Edit** or the name of the subzone). You can also configure the Default Subzone's **Authentication policy**. The policy is set to *Do not check credentials* by default.

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

H.323

Authentication 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 Cisco VCS is authoritative) or a non-local domain.

Authentication 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 a Cisco VCS is configured to use device authentication it will authenticate incoming SIP registration and INVITE requests. If the Cisco VCS then forwards the request on to a neighbor zone such as another Cisco 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 Cisco 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* [35]

The **Authentication trust mode** settings are:

- *On*: pre-authenticated messages are trusted without further challenge and subsequently treated as authenticated within the Cisco 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: you are recommended to enable authentication trust only if the neighbor zone is part of a network of trusted SIP servers.

Device authentication configuration

The **Device authentication configuration** page (**VCS configuration > Authentication > Devices > Configuration**) is used to control the type of database used by the Cisco VCS to store the authentication credentials used by systems and devices that attempt to communicate with the Cisco VCS.

Authentication database

To verify the identity of a device, the Cisco VCS needs access to a database on which all authentication credential information (usernames, passwords, and other relevant information) is stored. This database may be located either locally on the Cisco VCS, or on an LDAP Directory Server. The Cisco VCS looks up the endpoint's username in the database and retrieves the authentication credentials for that entry. If the credentials match those supplied by the endpoint, the registration is allowed to proceed.

The **Database type** setting determines which database the Cisco VCS uses during authentication:

- *Local database*: the local authentication database is used. You must configure the Local authentication database to use this option.
- *LDAP database*: a remote LDAP database is used. You must configure the LDAP server to use this option.

The default is *Local database*.

Note that:

- If the Cisco VCS is a traversal server, you must ensure that each traversal client's authentication credentials are entered into the selected database.
- The Cisco VCS supports the *ITU H.235* [1] specification for authenticating the identity of H.323 network devices with which it communicates.

Endpoint credentials used for authentication

An endpoint must supply the Cisco VCS with a username and password if it is required to authenticate with the Cisco 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**.

For details of how to configure endpoints with a username and password, please consult the endpoint manual.

Device authentication using LDAP

The **Device LDAP configuration** page (**VCS configuration > Authentication > Devices > LDAP configuration**) is used to configure a connection to the LDAP database used during device authentication.

Authentication process

If the Cisco VCS is using an LDAP server for authentication, the process is as follows:

1. The endpoint presents its username and authentication credentials (these are generated using its password) to the Cisco VCS, and the aliases with which it wants to register.
2. The Cisco VCS looks up the username in the LDAP database and obtains the authentication and alias information for that entry.

3. If the authentication credentials match those supplied by the endpoint, the registration will continue.

The Cisco VCS then determines which aliases the endpoint is allowed to attempt to register with, based on the **Alias origin** 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 LDAP database.

Configuring the LDAP server directory

The directory on the LDAP server should be configured to implement the *ITU H.350 specification* [2] to store credentials for devices with which the Cisco VCS communicates. The directory should also be configured with the aliases of endpoints that will register with the Cisco VCS. See LDAP configuration for device authentication for instructions on configuring LDAP servers.

LDAP server settings

The configurable options are:

Field	Description	Usage tips
LDAP server	The IP address or FQDN (or server address, if a DNS **Domain name** has also been configured) of the LDAP server.	
Port	The IP port of the LDAP server. Typically, non-secure connections use 389 and secure connections use 636. The default is 389.	
Encryption	Determines whether the connection to the LDAP server is encrypted using Transport Layer Security (TLS). ▪ *TLS*: TLS encryption is used for the connection to the LDAP server. ▪ *Off*: no encryption is used. The default is *Off*.	If you are connecting to an LDAP database using TLS encryption, you need to upload the trusted CA certificate for the LDAP server. Click **Upload a CA certificate file for TLS** to go to the Security certificates page.
User DN	The user distinguished name used by the Cisco VCS when binding to the LDAP server.	
Password	The password used by the Cisco VCS when binding to the LDAP server.	
Base DN	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.	

Field	Description	Usage tips
Alias origin	Determines how aliases are checked and registered. The options are: ▪ *LDAP*: for SIP registrations the AOR presented by the endpoint is registered providing it is listed in the LDAP database for the endpoint's username. For H.323 registrations: • At least one of the aliases presented by the endpoint must be listed in the LDAP database 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 LDAP database. Aliases presented by the endpoint that are not in the LDAP database will not be registered. • If no aliases are listed in the LDAP database, 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 LDAP database for its username. ▪ *Combined*: the aliases presented by the endpoint are used in addition to any listed in the LDAP database for the endpoint’s username. In other words, this is the same as for LDAP, except that if an endpoint presents an alias that is not in the LDAP database, it will be allowed to register with that alias. ▪ *Endpoint*: the aliases presented by the endpoint are used; any in the LDAP database are ignored. If no aliases are presented by the endpoint, it is not allowed to register. The default is *LDAP*.	When **Alias origin** is *LDAP*, MCUs are treated as a special case. They register with the presented aliases and ignore any aliases in the LDAP database. (This is to allow MCUs to additively register aliases for conferences.)

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

Note that if you want to use an LDAP database for device authentication, you must also go to the Authentication configuration page and select a **Database type** of *LDAP database*.

Device LDAP schemas

The **Device LDAP schemas** page (**VCS configuration > Authentication > Devices > LDAP schemas**) provides a set of .ldif files to be downloaded from the Cisco VCS and installed on the LDAP server.

Click **Download** to display the required schema in your browser from where you can use the browser's Save As command to store it on your file system.

See LDAP configuration for device authentication for more information.

Authentication using a local database

The **Local authentication database** page (**VCS configuration > Authentication > Devices > Local database**) page lists and allows you to manage the credentials stored in the local authentication database.

The local authentication database is included as part of your Cisco VCS system. The database can hold up to 2,500 credentials, each consisting of a **name** and **password**. These credentials are used for device, traversal client and TURN client authentication.

To add new credentials to the database, click **New**.

The maximum plaintext length for a password is 128 characters, which is then encrypted.

Note that:

- The same credentials can be used by more than one endpoint - you do not need to have a separate entry in the database for each endpoint.
- To use the local authentication database, you must select a **Database type** of *Local database* on the Device authentication configuration page.
- 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.

Authenticating with external systems

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

For example, when the Cisco VCS is forwarding an invite from an endpoint to another Cisco VCS, that other system may have authentication enabled and will therefore require your local Cisco 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 Cisco VCS (**VCS configuration > Zones**).

It includes the following information:

- an overview of your video communications network
- ways of structuring a dial plan
- an overview of the Local Zone and its subzones
- how to configure different zone types

About your video communications network

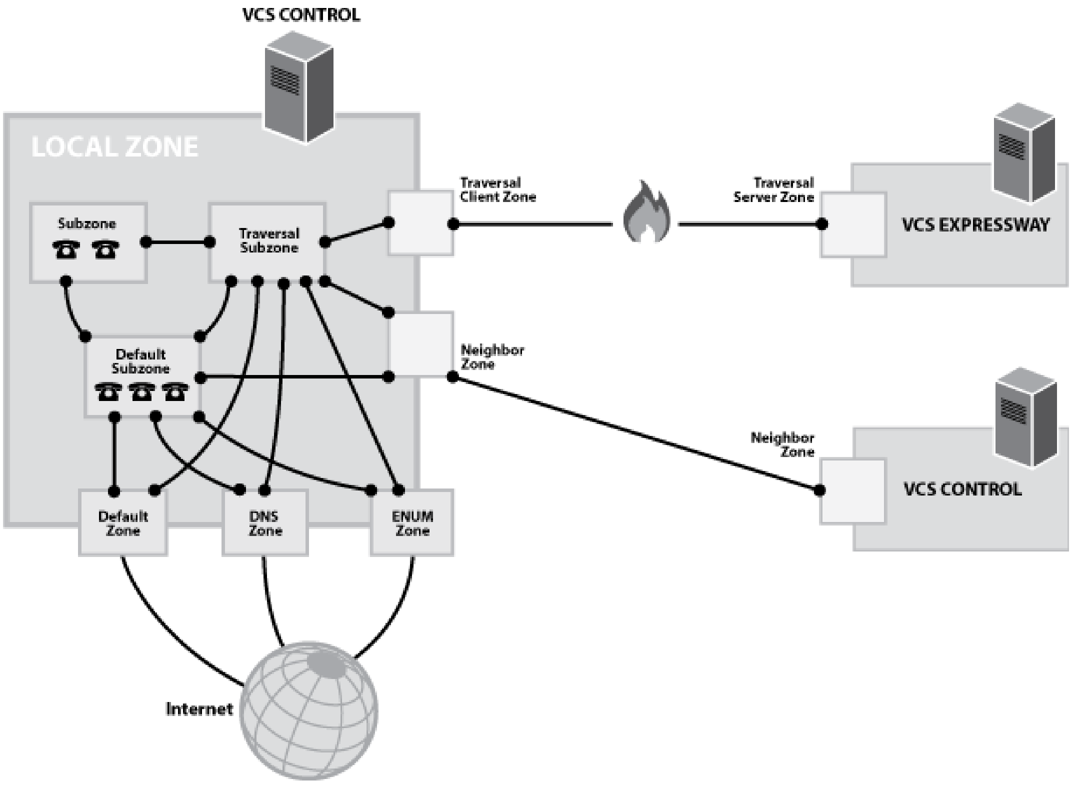
The most basic implementation of a video communications network is a single Cisco VCS connected to the internet with one or more endpoints registered to it. However, depending on the size and complexity of your enterprise the Cisco VCS may be part of a network of endpoints, other Cisco VCSs and other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

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

Example network diagram

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

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



Structuring your dial plan

As you start deploying more than one Cisco 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 Cisco 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 Cisco VCSs. Each Cisco VCS is then configured with all the other Cisco VCS as neighbor zones. When one Cisco 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 Cisco VCSs.

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

Hierarchical dial plan

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

The central Cisco VCS is configured with:

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

Each Cisco VCS is configured with:

- the central Cisco VCS as a neighbor zone
- a search rule with a **Mode** of *Any alias* and a **Target** of the central Cisco VCS

There is no need to neighbor the Cisco VCSs with each other. Adding a new Cisco VCS now only requires changing configuration on the new Cisco VCS and the central Cisco VCS.

However, failure of the central Cisco VCS in this situation could cause significant disruption to communications. Consideration should be given to the use of clustering for increased resilience.

Note: 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 Cisco 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).

About the Local Zone and subzones

The collection of all endpoints, gateways, MCUs and Content Servers registered with the Cisco 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 Cisco VCS it is allocated to an appropriate subzone based on subzone membership rules. These rules specify the range of IP addresses or alias pattern matches for each subzone. If an endpoint’s IP address or alias does not match any of the membership rules, it is assigned to the Default Subzone.

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

- the Traversal Subzone, which is always present
- the Cluster Subzone, which is always present but only used when your Cisco 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.

Local Zone searches

One of the functions of the Cisco 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 Cisco 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.

About zones

A zone is a collection of endpoints, either all registered to a single system (for example a Cisco VCS, Gatekeeper, or Border Controller), or located in a certain way such as via an ENUM or DNS lookup. Zones are used to:

- control through links whether calls can be made between 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 through the Cisco VCS's Authentication Policy

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 Cisco VCS.
- *Traversal client*: the local Cisco VCS is a traversal client of the system being connected to, and there is a firewall between the two.
- *Traversal server*: the local Cisco 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.

The Cisco 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.

Default Zone

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 are deemed to be coming from the Default Zone.

The Cisco VCS comes pre-configured with the Default Zone and default links between it and both the Default Subzone and the Traversal Subzone. The purpose of the Default Zone is to manage incoming calls from unrecognized endpoints to the Cisco VCS. You can do this by:

- deleting the default links; this prevents any incoming calls from unrecognized endpoints
- applying pipes to the default links; this lets you control the bandwidth consumed by incoming calls from unrecognized endpoints
- configuring the Default Zone's **Authentication Policy**

Note that the Default Zone cannot be deleted and its only configurable option is its **Authentication Policy** setting.

Zone configuration

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

To neighbor with another system (such as another Cisco VCS or gatekeeper), create a connection over a firewall to a traversal server or traversal client, or discover endpoints via an ENUM or DNS lookup, you must configure a zone on the local Cisco VCS. The Cisco VCS also has a pre-configured Default Zone which cannot be deleted.

When adding a new zone you must specify its **Type**. 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.

Note: connections between the Cisco 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 (**VCS configuration > Dial plan > Search rules**) otherwise search requests will not be sent to that zone.

Common zone configuration options

The zone configuration options depend upon the zone **Type**, however the following options apply to every zone type:

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

Configuring neighbor zones

A neighbor zone could be a collection of endpoints registered to another system (such as a Cisco VCS, Gatekeeper, or Border Controller), or it could be a SIP device (for example Microsoft Office Communications Server (OCS) 2007). 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 Cisco VCS. After you have added it, you can:

- query the neighbor about its endpoints
- apply transforms to any requests before they are sent to the neighbor
- control the bandwidth used for calls between your local Cisco VCS and the neighbor zone

Note that:

- neighbor zone relationship definitions are one-way; adding a system as a neighbor to your Cisco VCS does not automatically make your Cisco 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:

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 Cisco VCS. Select *Neighbor*.	After a zone has been created, the **Type** cannot be changed.
Hop count	The hop count is the number of times a request will be forwarded to a neighbor gatekeeper or proxy (see the Hop counts section for more information). This field specifies the hop count to use when sending a search request to this particular zone.	If the search request was received from another zone and already has a hop count assigned, the lower of the two values is used.
H.323 section:		
Mode	Determines whether H.323 calls are allowed to and from the neighbor system.	
Port	Specifies the port on the neighbor system used for H.323 calls from the local Cisco VCS.	This must be the same port number as that configured on the neighbor system as its H.323 UDP port. If the neighbor is another Cisco VCS, this is the port found under the **VCS configuration > Protocols > H.323** in the **Registration UDP Port** field.
SIP section:		
Mode	Determines whether SIP calls are allowed to and from the neighbor system.	
Port	Specifies the port on the neighbor system used for SIP connections from the local Cisco VCS.	This must be the same port number as that configured on the neighbor system as its SIP TCP, SIP TLS or SIP UDP listening port (depending on which SIP **Transport** mode is in use).

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 Cisco VCS performs X.509 certificate checking against the neighbor system when communicating over TLS.	If the neighbor system is another Cisco VCS, both systems can verify each other's certificate (known as mutual authentication). See TLS certificate verification of neighbor systems for more information.
Accept proxied registrations	Controls whether proxied SIP registrations routed through this zone are accepted.	This setting only applies to registration requests for a domain for which the Cisco 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.
Authentication section:		
Authentication policy	Controls how the Cisco 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 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 for more information.
Location section:		
Location Peer 1 to Peer 6 address	The IP address or FQDN of the neighbor system. If the neighbor is a Cisco VCS cluster, this includes all of the peers in the cluster.	See Neighboring the local Cisco VCS to another Cisco VCS cluster for more information.
Advanced section:		

Field	Description	Usage tips
Zone profile	Determines how the zone's advanced settings are configured. *Default*: uses the factory defaults. *Custom*: allows you to configure each setting individually. *Preconfigured profiles*: choose one of the preconfigured profiles to automatically use the appropriate settings required for connections to that type of system. The default is *Default*.	See Zone configuration: advanced settings for details on the *Advanced* settings. Do not use the *Custom* option or configure the individual *Advanced* settings except on the advice of Cisco customer support.

Configuring traversal client zones

To traverse a firewall, the Cisco VCS must be connected with a traversal server (for example a Cisco VCS Expressway or a TANDBERG Border Controller).

In this situation your local Cisco VCS is a traversal client, so you create a connection with the traversal server by creating a traversal client zone on your local Cisco 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 Cisco VCS client zone.)

After you have neighbored with the traversal server you can:

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

For full details on how traversal client zones and traversal server zones work together to achieve firewall traversal, see About firewall traversal.

An NTP server must be configured for traversal zones to work.

The configurable options for a traversal client zone are:

Field	Description	Usage tips
Configuration section:		
Name	The name acts as a unique identifier, allowing you to distinguish between zones of the same type.	
Type	The nature of the specified zone, in relation to the local Cisco 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.

Field	Description	Usage tips
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 on a Cisco VCS, 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 Firewall traversal protocols and ports for more information.
Port	The port on the traversal server to use for H.323 calls to and from the local Cisco VCS.	For firewall traversal to work via H.323, the traversal server must have a traversal server zone configured on it to represent this Cisco 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 Cisco VCS. This must be different from the listening ports used for incoming TCP, TLS and UDP SIP calls (typically 5060 and 5061).	For firewall traversal to work via SIP, the traversal server must have a traversal server zone configured on it to represent this Cisco 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*.	
TLS verify mode	Controls X.509 certificate checking and mutual authentication between this Cisco VCS and the traversal server when communicating over TLS.	See TLS certificate verification of neighbor systems for more information.
Accept proxied registrations	Controls whether proxied SIP registrations routed through this zone are accepted.	This setting only applies to registration requests for a domain for which the Cisco 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.

Field	Description	Usage tips
Poison mode	Determines if SIP requests sent to systems located via this zone are "poisoned" such that if they are received by this Cisco VCS again they will be rejected.	
Authentication section:		
Authentication policy	Controls how the Cisco 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 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 Cisco VCS Expressway cluster, this should include all of its peers. ▪ If the traversal server is a TANDBERG Border Controller, this should include all its Alternates.	See Neighboring the local Cisco VCS to another Cisco VCS cluster for more information.

Configuring traversal server zones

A Cisco VCS Expressway is able to act as a traversal server, providing firewall traversal on behalf of traversal clients (for example, Cisco VCS Controls or gatekeepers).

To act as a traversal server, the Cisco VCS Expressway must have a special type of two-way relationship with each traversal client. To create this connection, you create a traversal server zone on your local Cisco VCS Expressway and configure it with the details of the corresponding zone on the traversal client. (The client must also be configured with details of the Cisco VCS Expressway.)

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 Cisco VCS and the traversal client

Note: traversal client-server zone relationships must be two-way. For firewall traversal to work, the traversal server and the traversal client must each be configured with the other's details (see Quick guide to Cisco VCS traversal client - server configuration for more information). The client and server will then be able to communicate over the firewall and query each other. For full details on how traversal client zones and traversal server zones work together to achieve firewall traversal, see About firewall traversal.

An NTP server must be configured for traversal zones to work.

The configurable options for a traversal server zone are:

Field	Description	Usage tips
Configuration section:		
Name	The name acts as a unique identifier, allowing you to distinguish between zones of the same type.	
Type	The nature of the specified zone, in relation to the local Cisco 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 Cisco VCS Expressway. ▪ If the traversal client is a Cisco VCS, this must be its connection credentials **Username** as configured in its traversal client zone. ▪ If the traversal client is a TANDBERG Gatekeeper, this is its **System Name**.	There must also be an entry in the Cisco 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 **VCS 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 Firewall traversal protocols and ports for more information.
Port	The port on the local Cisco VCS Expressway to use for H.323 calls to and from the traversal client.	

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 Cisco 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*.	
TLS verify mode and **subject name**	Controls X.509 certificate checking and mutual authentication between this Cisco 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.	See TLS certificate verification of neighbor systems for more information.
Accept proxied registrations	Controls whether proxied SIP registrations routed through this zone are accepted.	This setting only applies to registration requests for a domain for which the Cisco 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.
Poison mode	Determines if SIP requests sent to systems located via this zone are "poisoned" such that if they are received by this Cisco VCS again they will be rejected.	
Authentication section:		

Field	Description	Usage tips
Authentication policy	Controls how the Cisco 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 for more information.
UDP / TCP probes section:		
UDP retry interval	The frequency (in seconds) with which the client sends a UDP probe to the Cisco 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 Cisco VCS Expressway during call setup.	
UDP keep alive interval	The interval (in seconds) with which the client sends a UDP probe to the Cisco 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 Cisco 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 Cisco VCS Expressway during call setup.	
TCP keep alive interval	The interval (in seconds) with which the traversal client sends a TCP probe to the Cisco 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 Cisco VCS and each group of ENUM endpoints

Full details of how to use and configure ENUM zones are given in the About ENUM dialing section.

The configurable options for an ENUM zone are:

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 Cisco 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 endpoints' aliases.

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

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

See About URI dialing for more information on configuring and using DNS zones.

The configurable options for a DNS zone are:

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 Cisco VCS. Select *DNS*.	After a zone has been created, the **Type** cannot be changed.

Field	Description	Usage tips
Hop count	The hop count is the number of times a request will be forwarded to a neighbor gatekeeper or proxy (see the Hop counts section for more information). This field specifies the hop count to use when sending a search request to this particular zone.	If the search request was received from another zone and already has a hop count assigned, the lower of the two values is used.
H.323 mode	Determines whether H.323 calls are allowed to systems and endpoints located using DNS lookups via this zone.	
SIP mode	Determines whether SIP calls are allowed to systems and endpoints located using DNS lookups via this zone.	
TLS verify mode	Controls whether the Cisco VCS performs X.509 certificate checking against the destination system server returned by the DNS lookup.	This setting only applies if the DNS lookup specifies TLS as the required protocol. If TLS is not required then the setting is ignored. See TLS certificate verification of neighbor systems for more information.
Zone profile	Determines how the zone's advanced settings are configured. *Default*: uses the factory defaults. *Custom*: allows you to configure each setting individually. *Preconfigured profiles*: choose one of the preconfigured profiles to automatically use the appropriate settings required for connections to that type of system. The default is *Default*.	See Zone configuration: advanced settings for details on the *Advanced* settings. Do not use the *Custom* option or configure the individual *Advanced* settings except on the advice of Cisco customer support.

Zone configuration: advanced settings

The table below describes the *Advanced* and *Custom* zone configuration options. Some of these settings only apply to specific zone types.

Note: you should only use the *Custom* zone profile settings on the advice of Cisco customer support.

Setting	Description	Default	Applicable to
Zone profile	Determines how the zone's advanced settings are configured. *Default*: uses the factory defaults. *Preconfigured profiles*: alternatively, choose one of the preconfigured profiles to automatically use the appropriate settings required for connections to that type of system. The options include: - *Microsoft Office Communications Server 2007*: (see the *Cisco VCS Control interworking with Microsoft OCS* deployment guide [24] for more information) - *Cisco Unified Communications Manager* (see the *Cisco Unified Communications Manager with Cisco VCS using a SIP trunk* deployment guide [36] for more information) - *Nortel Communication Server 1000* - *Cisco Advanced Media Gateway* (see the *Microsoft OCS 2007, Cisco VCS Control and Cisco AM GW* deployment guide [37] for more information) - *Non-registering device* (typically used for non-gatekeeper devices such as an MCU) *Custom*: allows you to configure each *Advanced* setting individually. These settings are listed in the remainder of this table below.	Default	Neighbor zones DNS zones
Monitor peer status	Specifies whether the Cisco 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 zones
H.323 searches are automatically responded to	Determines what happens when the Cisco 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 zones

Setting	Description	Default	Applicable to
SIP searches are automatically responded to	Determines what happens when the Cisco 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 option should normally be left as the default *Off*. However, some systems such as Microsoft Office Communications Server (OCS) 2007 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 zones DNS zones
Empty INVITE allowed	Determines whether the Cisco 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 systems such as Microsoft OCS 2007 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] DNS Interworking SIP** commands. They should only be changed on the advice of Cisco customer support.	On	Neighbor zones DNS zones
SIP poison mode	*On*: SIP requests sent to systems located via this zone are "poisoned" such that if they are received by this Cisco VCS again they will be rejected. *Off*: SIP requests sent out via this zone that are received by this Cisco VCS again will not be rejected; they will be processed as normal.	Off	Neighbor zones Traversal clients Traversal servers DNS zones

Setting	Description	Default	Applicable to
SIP encryption mode	Determines whether or not the Cisco 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*. However, this must be set to *Microsoft* for Microsoft Office Communications Server (OCS) 2007 zones.	Auto	Neighbor zones
SIP SDP attribute line limit mode	Determines whether requests containing SDP sent out to this zone have the length of **a=fmtp** lines restricted. *On*: the length is truncated to the maximum length specified by the SIP SDP attribute line limit length setting. *Off*: the length is not truncated. The **SIP SDP attribute line limit** option should normally be left as the default of *Off*. However, some systems such as Microsoft OCS 2007 cannot handle attribute lines longer than 130 characters, so it must be set to *On* for connections to these systems.	Off	Neighbor zones DNS zones
SIP SDP attribute line limit length	If **SIP SDP attribute line limit mode** is set to *On*, sets the maximum line length of **a=fmtp** SDP lines.	130	Neighbor zones DNS zones
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*. However, it must be set to *On* for connections to a Microsoft OCS 2007 Release 2 system.	Off	Neighbor zones
SIP UPDATE strip mode	Controls whether or not the Cisco 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 such as Microsoft OCS 2007 do not support the UPDATE method in the Allow header, so for these zones this should be set to *On*.	Off	Neighbor zones

Setting	Description	Default	Applicable to
Interworking SIP search strategy	Determines how the Cisco VCS searches for SIP endpoints when interworking an H.323 call. *Options*: the Cisco VCS sends an OPTIONS request. *Info*: the Cisco VCS sends an INFO request. This option should normally be left as the default *Options*. However, some endpoints such as Microsoft Office Communicator (MOC) clients cannot respond to OPTIONS requests, so this must be set to *Info* for connections to a Microsoft OCS 2007 system.	Options	Neighbor zones
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, so this must be set to *On* for connections to a Cisco Unified Communications Manager. *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 zones DNS zones
SIP Duo Video filter mode	Determines whether INVITE requests sent to this zone filter out Duo Video. This option may be required to enable interoperability with SIP devices that do not support Duo Video, so this must be set to *On* for connections to a Cisco Unified Communications Manager. *On*: the second video line in any outgoing INVITE request is removed. *Off*: INVITE requests are not modified.	Off	Neighbor zones DNS zones
SIP record route address type	Controls whether the Cisco 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 Cisco VCS's IP address. *Hostname*: uses the Cisco VCS's **Local host name** (if it is blank the IP address is used instead).	IP	Neighbor zones DNS zones
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 zones

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

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	Microsoft Office Communications Server 2007	Cisco Unified Communications Manager	Nortel Communication Server 1000	Cisco Advanced Media Gateway	Non-registering device
Monitor peer status	Yes	Yes	Yes	Yes	No
H.323 searches are automatically responded to	Off	Off	Off	Off	On
SIP searches are automatically responded to	Off	Off	Off	Off	On
Empty INVITE allowed	Off	On	On	On	On
SIP poison mode	On	Off	Off	Off	Off
SIP encryption mode	Microsoft	Auto	Auto	Auto	Auto
SIP SDP attribute line limit mode	On	Off	Off	Off	Off

Setting	Microsoft Office Communications Server 2007	Cisco Unified Communications Manager	Nortel Communication Server 1000	Cisco Advanced Media Gateway	Non-registering device
SIP SDP attribute line limit length	130	130	130	130	130
SIP multipart MIME strip mode	On	Off	Off	Off	Off
SIP UPDATE strip mode	On	On	On	On	Off
Interworking SIP search strategy	Info	Options	Options	Options	Options
SIP UDP/BFCP filter mode	Off	On	Off	Off	Off
SIP Duo Video filter mode	On	Off	Off	Off	Off
SIP record route address type	Hostname	IP	IP	IP	IP
SIP Proxy-Require header strip list	<blank>	<blank>	"com. nortelnetworks. firewall"	<blank>	<blank>

TLS certificate verification of neighbor systems

When a SIP TLS connection is established between a Cisco VCS and a neighbor system, the Cisco 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 verification is enabled, the neighbor system's FQDN or IP address, as specified in the **Peer address** field of the zone's configuration, is used to verify against the certificate holder's name contained within the X.509 certificate presented by that system. (The name has to be contained in either the Subject Common Name or the Subject Alternative Name attributes of the certificate.) The certificate itself must also be valid and signed by a trusted certificate authority.

Note that for traversal server 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 Cisco 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 Cisco VCS acts both as a client and as a server and therefore you must ensure that each Cisco VCS's certificate is valid both as a client and as a server.

See the Managing security certificates section for more information about certificate verification and for instructions on uploading the Cisco VCS's server certificate and uploading a list of trusted certificate authorities.

Clustering and peers

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

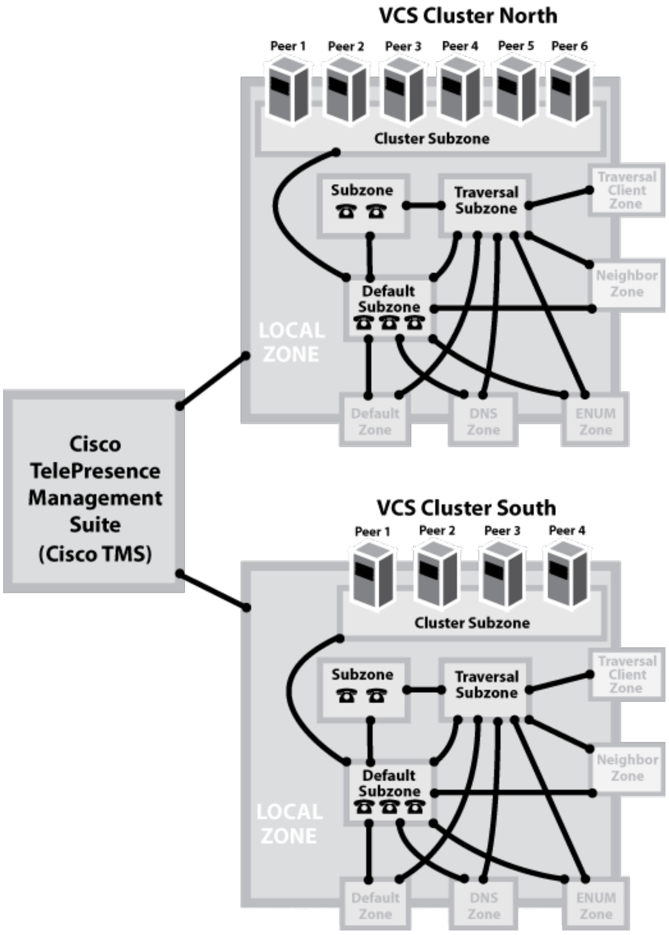
- an overview of clustering
- guidelines for setting up and maintaining a cluster
- a list of configuration that is not replicated across cluster peers
- a troubleshooting guide for cluster replication problems
- how registrations and bandwidth are shared across peers
- how clustering works with FindMe, Presence and Cisco TMS
- the purpose of the cluster subzone
- how to neighbor a local Cisco VCS or cluster to a remote Cisco VCS cluster

About clusters

A Cisco VCS can be part of a cluster of up to six Cisco VCSs. Each Cisco VCS in the cluster is a peer of every other Cisco VCS in the cluster. When creating a cluster, you define a cluster name and nominate one peer as the master from which all relevant configuration is replicated to the other peers in the cluster. Clusters are used to:

- increase the capacity of your Cisco VCS deployment compared with a single Cisco VCS
- provide redundancy in the rare case that a Cisco VCS becomes unavailable (for example, due to a network or power outage)

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



About the configuration master

All peers in a cluster must be configured identically for subzones, zones, links, pipes, authentication, bandwidth control and Call Policy. To achieve this, you define a cluster name and nominate one peer as the configuration master. Any configuration changes made to the master peer are then automatically replicated across all the other peers in the cluster.

You should make configuration changes on the master Cisco VCS. Any changes made on other peers are not reflected across the cluster, and will be overwritten the next time the master's configuration is replicated across the peers. The only exceptions to this are:

- some specific configuration items that are not replicated
- user account details (you can maintain these on any peer)

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

Secure communication between peers

The Cisco VCS uses IPsec (Internet Protocol Security) to enable secure communication between each cluster peer. Authentication is carried out through the use of a pre-shared access key.

Each peer in the cluster must be configured with the IP address and associated access key of every other peer in that cluster.

Alternates

"Alternate" is an H.323 term for a system used to provide redundancy to a Primary gatekeeper, and prior to version X3.0 the Cisco VCS supported Alternates. From X3.0 onwards, redundancy (along with other features) is provided by clusters of peers, which support both H.323 and SIP and work as equals. However, peers may sometimes be referred to as Alternates. Also note that some versions of Cisco TMS refer to peers as "members".

Setting up a cluster

Before creating your cluster, ensure that all the Cisco VCSs to be added to the cluster:

- are using Cisco TMS version 12.6 or later as their external manager
- have the same software version and option keys installed
- each have a different system name
- are configured with a working NTP server
- each have a different LAN configuration (a different IPv4 address and a different IPv6 address, where enabled)
- have H.323 enabled (even if all endpoints in the cluster are SIP only, H.323 signaling is used for endpoint location searching and sharing bandwidth usage information with other peers in the cluster)
- have SSH enabled (data replication between peers uses SSH)
- have access to the root account via SSH enabled

Then, to create your cluster you must first configure a master peer and then add the other peers into the cluster one-by-one.

You are recommended to backup your Cisco VCS data before setting up a cluster.

A full step-by-step guide on using the clustering script and configuring clusters is available in the *Cluster creation and maintenance* deployment guide [27].

Maintaining a cluster

The **Clustering** page (**VCS configuration > Clustering**) lists the IP addresses of all the peers in the cluster, to which this Cisco VCS belongs, and identifies the master peer.

Cluster name

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

If you are using FindMe and you change the **Cluster name**, you may need to reconfigure the user accounts. See the Clustering and FindMe section for further details.

Cluster pre-shared key

The Cisco VCS uses IPsec (Internet Protocol Security) to enable secure communication between each cluster peer.

The **Cluster pre-shared key** is the common IPsec access key used by each peer to access every other peer in the cluster.

- Each peer in the cluster must be configured with the same **Cluster pre-shared key**.

Setting configuration for the cluster

You should make configuration changes on the master Cisco VCS. Any changes made on other peers are not reflected across the cluster, and will be overwritten the next time the master's configuration is replicated across the peers. The only exceptions to this are:

- some specific configuration items that are not replicated
- user account details (you can maintain these on any peer — FindMe data uses a different replication mechanism)

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. Instructions for this are contained in the *Cluster creation and maintenance* deployment guide [27].

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

If peers are deployed on different LANs, there must be sufficient connectivity between the networks to ensure a low degree of latency between the peers - a maximum delay of 15ms one way, 30ms round-trip.

Deploying all peers in a cluster on the same LAN means they can be configured with the same routing information such as local domain names and local domain subnet masks.

Changing the master peer

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

- the original master peer fails
- you want to take the master Cisco VCS unit out of service

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

To change the master peer you must log in to every other Cisco VCS in the cluster and change the configuration master on each peer:

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

Note that during this process you may see warning messages raised on some peers about inconsistent master peer configuration. These warnings will be lowered when every peer in the cluster is configured with the new master.

Monitoring the status of the cluster

The status sections at the bottom of the **Clustering** page show you the current status of the cluster, and the time of the previous and next synchronization. From here you can also go to the **TMS Agent replication status** page. This shows the current status of the TMS Agent service and can be used to assist in troubleshooting replication problems.

Configuration that is not replicated across a cluster

Most items of configuration are replicated from the master to all peers, with the exceptions listed below.

System name

The system name is not replicated. It must be different for each peer in the cluster.

Administrator accounts

The password for the default **admin** administrator account is not replicated. Each peer can have a different password. Any other administrator accounts and passwords will be replicated from the master peer to all other peers.

Option keys

Option keys are not replicated. Each peer must have an identical set of option keys installed, but you must purchase these separately for each peer in the cluster.

Ethernet speed

The Ethernet speed is not replicated. Each peer may have slightly different requirements for the connection to their Ethernet switch.

IP configuration

LAN configuration is not replicated across peers. Each peer must have a different IPv4 address and a different IPv6 address.

- IP gateway configuration is not replicated. Each peer can use a different gateway.
- IP routes (also known as static routes) are not replicated. If these are used, they can be different for each peer.

Note that the IP protocol is replicated, because each peer must support the same protocols.

DNS configuration

DNS servers are not replicated across peers - each peer can use a different set of DNS servers. However, the DNS domain name is replicated across peers.

Logging

The Event Log and Configuration Log on each peer will only report activity for that particular Cisco VCS. You are recommended to set up a remote syslog server to which the logs of all peers can be sent. This will allow you to have a global view of activity across all peers in the cluster. See the logging section for further details.

Conference Factory template

The template used by the Conference Factory application to route calls to the MCU is not replicated, as it must be unique for each peer in the cluster.

CA certificates

The security certificates and certificate revocation lists (CRLs) used by the Cisco VCS must be uploaded individually per peer.

Note: configuration data that is replicated across peers should not be modified on non-master peers. At best it will result in the changes being overwritten from the master; at worst it will cause cluster replication to fail.

Troubleshooting cluster replication problems

Cluster replication can fail for a variety of reasons. The most common problems are listed below, followed by instructions for resolving the problem:

NTP servers not configured and active on each cluster peer

1. For each peer in the cluster, go to the **System > Time** page.
2. Ensure the peer has a correctly configured and active **NTP server**.

Some peers have a different master peer defined

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

Cluster configuration script has not been run against each peer

1. For each peer in the cluster, go to the **VCS configuration > Clustering** page.
2. Enter the address of each of peer into the **Peer IP address** fields and configure the **Configuration master**. Ensure each peer identifies the same **Configuration master** peer.
3. Log in to each peer as **root** (by default you can only do this using a serial connection or SSH) and run the cluster configuration script. Full details on running this script and configuring clusters is available in the *Cluster creation and maintenance* deployment guide [27].

Note that cluster replication warnings can appear briefly while the cluster is initially being set up. These warnings are removed after the data has completed synchronizing and the cluster has stabilized. This takes approximately 3 minutes.

Unable to reach the cluster configuration master peer

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

- network access problems
- Cisco VCS unit is powered down
- incorrectly configured IP addresses
- incorrectly configured IPsec keys - ensure each peer is configured with the same **Cluster pre-shared key** value.

"Manual synchronization of configuration is required" warnings are raised on peer Cisco VCSs

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

This will delete the non-master Cisco VCS configuration and force it to update its configuration from the master Cisco VCS.

CAUTION: never issue this command on the master Cisco VCS, otherwise all configuration for the cluster will be lost.

Managing clusters and peers

Sharing registrations across peers

When one Cisco VCS in a cluster receives a search request (such as an LRQ, ARQ or an INVITE), it checks its own and its peers' registration databases before responding. This allows all endpoints in the cluster to be treated as if they were registered with a single Cisco 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.

Note: when using a cluster, you should change the registration **Time to live** on all peers in the cluster from the default 30 minutes to just a few minutes. This setting determines how often endpoints are required to re-register with their Cisco VCS, and reducing this to just a few minutes ensures that if one Cisco VCS becomes unavailable, the endpoint will quickly failover to one of its peers. To change this setting, go to **VCS configuration > Protocols > H.323 > Gatekeeper > Time to live**.

SIP registrations

Failover re-registration to a peer applies to H.323 re-registrations only.

The SIP standard currently has no direct equivalent, but some SIP UAs including Movi™ v2.0 (or later) clients support similar functionality. If you configure such endpoints with a SIP server address that is an FQDN, and configure this FQDN to resolve 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 was 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 Cisco VCS manages bandwidth, see the bandwidth control section.

Cluster upgrades and downgrades

The clustering feature was introduced to the Cisco VCS in software release X3.0.

Upgrading from versions prior to X3.0

If you are upgrading from Cisco VCS software versions prior to X3.0 and want to implement clustering, you must:

1. Remove any existing Alternate configuration.
2. Upgrade all Cisco VCSs to be added to the cluster to the latest Cisco VCS software version.
3. Follow the steps outlined in Setting up a cluster.

Downgrading

See the Upgrade procedure section for details on restoring system configuration details.

Cluster backup and restore

The backup and restore process can be used to save and restore cluster configuration information.

Backing up a cluster

The backup process saves all configuration information for the cluster, regardless of the Cisco VCS used to make the backup.

Restoring a cluster

You cannot restore data to a Cisco VCS that is a part of a cluster.

To restore previously backed up cluster configuration data you must follow this process:

1. Remove a Cisco VCS peer from the cluster so that it becomes a standalone Cisco VCS.
2. Restore the configuration data to the standalone Cisco VCS.
3. Build a new cluster using the Cisco 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 for more information about adding and removing cluster peers.

Clustering and FindMe

Clustering supports the use of FindMe. Each peer has its own FindMe database containing all user account information for the cluster. When a user account is created or edited on one peer, that peer shares the information about the changes to all other peers in the cluster, which then update their own FindMe databases accordingly.

Note: there is a limit of 10,000 FindMe user accounts per Cisco VCS cluster. Multiple clusters are required if you have more than 10,000 users.

The replication of FindMe database information uses a different mechanism (the TMS Agent) to that used to replicate configuration information. Configuration information must be changed on the master peer only, but changes to FindMe information can be made on any peer and will be shared with all other peers.

If you are part of a large enterprise with, for example, Cisco TMS managing several Cisco VCS clusters, the FindMe database may contain details of users and devices in other Cisco VCS clusters. Different clusters are distinguished by their **Cluster name** (see below). You cannot modify the details of accounts that are not managed in your cluster.

Cluster name

You must define a **Cluster name** if you are using FindMe, even if the Cisco VCS is not part of a cluster.

If you change the cluster name after creating your user accounts you will have to reconfigure those accounts to associate them with the new cluster name. You can do this by running the **transferfindmeaccounts** script. Instructions for how to do this are contained in the *FindMe* deployment guide [29].

Alternatively, if you try to edit an account that belongs in a different cluster the system gives you an option to **Move this account to local cluster**. Selecting this option updates that particular account so that it now belongs to your local Cisco VCS cluster and hence lets you edit that account's details. See Maintaining a cluster for more information on configuring the cluster name.

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 Cisco VCS only.
- **Subscribers** shows each endpoint from which a subscription request has been received on the local Cisco VCS only.

Clustering and Cisco TMS

You are recommended to use Cisco TMS when running a cluster of Cisco VCSs. For full information, refer to the Cisco TMS documentation.

- Cisco TMS (version 12.5 or later) is mandatory if your cluster is configured to use FindMe or Device Provisioning.

If you were using Cisco TMS to manage a cluster running a version of the Cisco VCS software prior to X5, refer to the *Cluster creation and maintenance* deployment guide [27] for upgrade instructions.

In previous Cisco VCS releases, replication between peers was managed by Cisco TMS. From Cisco VCS version X4 onwards, replication is managed by the Cisco VCSs themselves.

About the Cluster Subzone

When two or more Cisco 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 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 Cisco VCS for the Branch Office, which is neighbored to a cluster of 4 Cisco 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 routed mode** is set to *Optimal* and the call is H.323, the call will not appear on Peer 2, and on Peer 1 the route will be **Branch Office > DefaultSubzone**.

Neighboring the local Cisco VCS to another Cisco VCS cluster

You can neighbor your local Cisco VCS (or Cisco VCS cluster) to a remote Cisco VCS cluster; this remote cluster could be a neighbor, traversal client, or traversal server to your local Cisco VCS. In this case, when a call is received on your local Cisco 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)

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

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

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

Configuration

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

Note that:

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

TMS Agent replication status

The **TMS Agent replication status** page (**VCS configuration > Clustering** and then click **View TMS Agent replication status**) shows the current status of the TMS Agent service.

The status report is used to assist in troubleshooting replication problems. It lists each Cisco TMS and Cisco VCS server peer whose data (FindMe and Device Provisioning, and not Cisco VCS configuration) is being replicated between themselves by the TMS Agent service.

For each server the report indicates:

- the number of changes still to replicated to that server (and that have been applied to at least one of the other servers)
- the date of the oldest change still to be applied to that server
- the port number being used for replication communication between the servers and whether that communication is encrypted or not

Note that the TMS Agent replication status is only relevant if the Cisco VCS has the FindMe or Device Provisioning option keys enabled (as the TMS Agent service is not required otherwise).

Dial plan and call processing

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

This section includes:

- an overview of the Cisco VCS's call routing process
- how hop counts affect the search process
- how to configure the Cisco VCS's dial plan options
- the pre-search transform process
- the search and zone transform process
- how to use Call Policy to manage calls
- routing calls via the Cisco TelePresence Advanced Media Gateway
- the different address dial formats that can be used to initiate a call
- how to set up your network to handle incoming and outgoing calls made via URI dialing and ENUM dialing
- call signaling configuration options
- how to identify calls
- how to disconnect calls

Call routing process

One of the functions of the Cisco 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 Cisco 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.

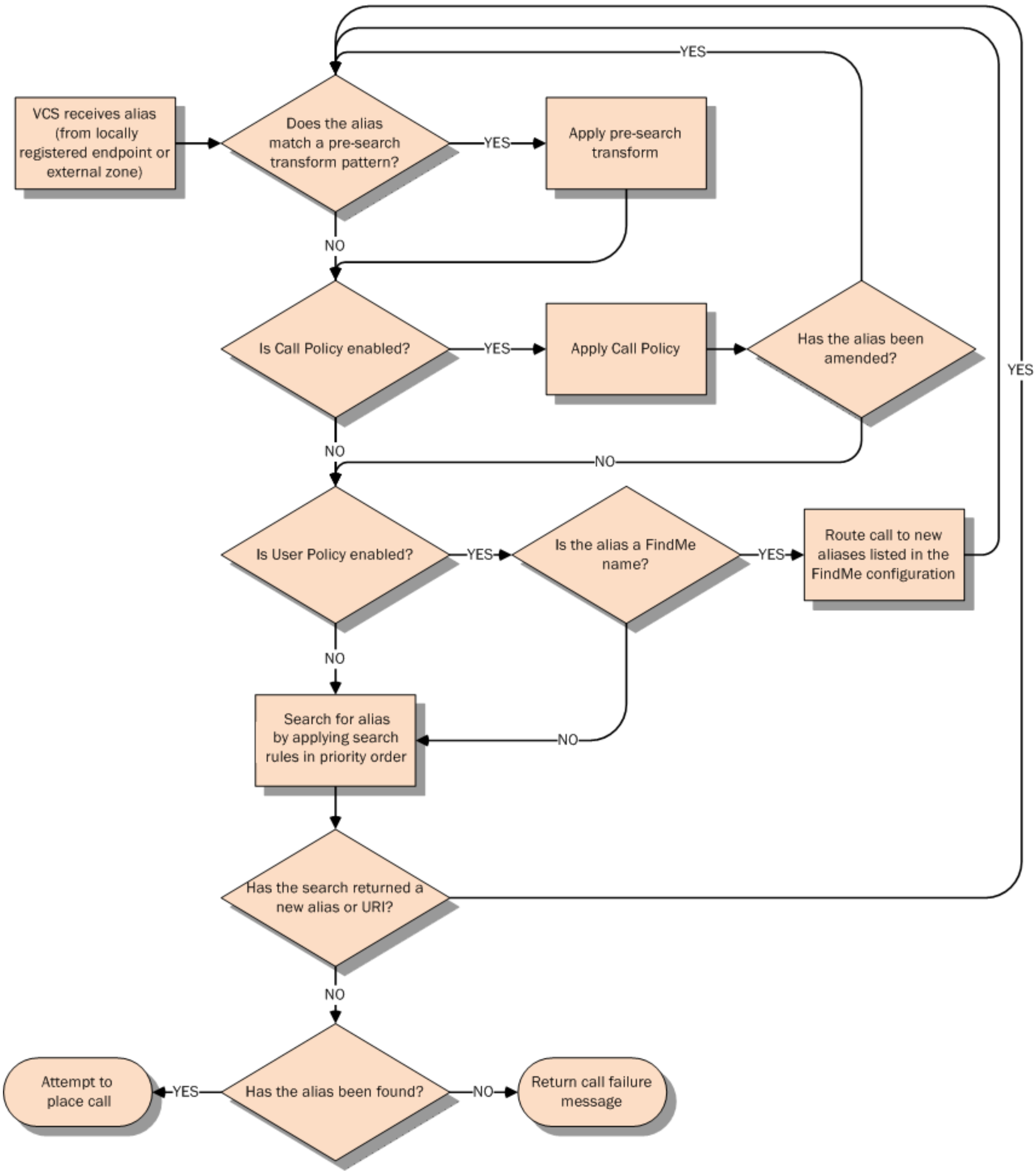
How the Cisco VCS determines the destination of a call

The process followed by the Cisco 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 sent from the caller’s endpoint to its local Cisco VCS (the Cisco VCS to which it is registered).
3. Any pre-search transforms are applied to the alias.
4. Any Call Policy is applied to the (transformed) alias. If this results in a new alias, the process starts again with the new alias 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 aliases, the process starts again with all the resulting aliases checked against pre-search transforms and Call Policy.
6. The Cisco VCS then searches for the alias according to its search rules:
    - A matching rule may apply a zone transform to the alias before sending the query on to its **Target**. A **Target** can be one of the following types:

- **Local Zone**: the endpoints and devices registered to the Cisco VCS.
- **Neighbor zone**: one of the Cisco VCS's configured external neighbor zones, or a DNS or ENUM lookup zone.
- **Policy service**: an external service or application, such as a Conference Factory. 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 an 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 Cisco 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 Cisco 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.


VCS receives alias (from locally registered endpoint or external zone)
Does the alias match a pre-search transform pattern?
YES
Apply pre-search transform
YES
NO
Is Call Policy enabled?
YES
Apply Call Policy
Has the alias been amended?
YES
NO
NO
Is User Policy enabled?
YES
Is the alias a FindMe name?
YES
Route call to new aliases listed in the FindMe configuration
NO
NO
Search for alias by applying search rules in priority order
Has the search returned a new alias or URI?
NO
Attempt to place call
YES
Has the alias been found?
NO
Return call failure message

About the Cisco VCS's directory service

The Cisco VCS's directory service is an on-box repository of dial plan information. It contains call routing information and can provide registration and call policy services.

The directory service has no user configurable options on the Cisco VCS. The dial plan and policy information is managed on a separate dial plan server and its contents are be pushed out to all of its client Cisco VCSs. It is suited to large-scale deployments where a centrally-managed system can provide a comprehensive directory of aliases and their corresponding routing information.

You can configure the Cisco VCS to use the directory service in the following areas:

- Registration restriction policies: as an alternative to using Allow and Deny Lists
- Call Policy configuration: where it can be applied in addition to locally-defined Call Policy

About 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 Cisco 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 Cisco 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

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

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

For full details on other zone options, see the Zone configuration section.

About transforms and search rules

The Cisco 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 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 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 Cisco 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 source of the query (such as the Local Zone, or any known zone)
- 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 Cisco 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 Cisco VCS may then search the same zone again using the alternative protocol, depending on where the search came from and the **Interworking mode** (**VCS configuration > Protocols > Interworking**):

- If the request has come from a neighboring system and **Interworking mode** is set to *Registered only*, the Cisco 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 Cisco VCS searches the Local Zone and all external zones using both protocols.

Dial plan configuration

The **Dial plan configuration** page (**VCS configuration > Dial plan> Configuration**) is used to configure how the Cisco VCSroutes calls in specific call scenarios.

The configurable options are:

Field	Description	Usage tips
Calls to unknown IP addresses	Determines the way in which the Cisco 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 Cisco 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 Cisco 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 Cisco VCS may only call an IP address of a system also registered directly to that Cisco 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 the IP dialing section for more information.
Fallback alias	The alias to which incoming calls are placed for calls where the IP address or domain name of the Cisco 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 Cisco 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 Cisco VCS directly
- the caller has dialed a domain name belonging to the Cisco VCS (either one of its configured SIP domains, or any domain that has an SRV record that points at the IP address of the Cisco 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 Cisco 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 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 Cisco 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 Cisco 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. A Cisco VCS in a cluster 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 (**VCS configuration > Dial plan > Transforms**) lists all the pre-search transforms currently configured on the Cisco 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 **Behavior** and **Replace** rules.

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

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

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**).
Pattern string	Specifies the pattern against which the alias is compared.	
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*.

Field	Description	Usage tips
State	Indicates if the transform is enabled or not.	When you are making or testing configuration changes to your transforms, you may want to temporarily enable or disable certain transforms. You can do this by selecting the transform's check box and clicking **Enable** or **Disable** as appropriate. Any disabled transforms still appear in the transforms list but are ignored by the Cisco VCS when processing search requests.

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 Cisco 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 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 Cisco VCS from searching any other zones unnecessarily.

Configuring search rules

The **Search rules** page (**VCS configuration > Dial plan > Search rules**) is used to configure how the Cisco 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.

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.
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.	
Request must be authenticated	Specifies whether the search rule applies only to authenticated search requests.	This can be used in conjunction with the Cisco VCS's Authentication Policy to limit the set of services available to unauthenticated devices.

Field	Description	Usage tips
Mode	The method used to test if the alias applies to the search rule. *Alias pattern match*: the alias must match the specified **Pattern type** and **Pattern string**. *Any alias*: any alias (providing it is not an IP address) is allowed. *Any IP Address*: the alias must be an IP address.	
Pattern type	How the **Pattern string** must match the alias for the rule to be applied. Options are: *Exact*: the entire string must exactly match the alias character for character. *Prefix*: the string must appear at the beginning of the alias. *Suffix*: the string must appear at the end of the alias. *Regex*: treats the string as a regular 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*.
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.

Field	Description	Usage tips
On successful match	Controls the ongoing search behavior if the alias matches the search rule. *Continue*: continue applying the remaining search rules (in priority order) until the endpoint identified by the alias is found. *Stop*: do not apply any more search rules, even if the endpoint identified by the alias is not found in the target zone.	If *Stop* is selected, any rules with the same priority level as this rule are still applied.
Target	The zone or policy service to query if the alias matches the search rule.	You can configure external 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 Conference Factory. The service will return some CPL which could, for example, specify a new destination alias which would start the search process over again.
State	Indicates if the search rule is enabled or not.	When you are making or testing configuration changes to your search rules, you may want to temporarily enable or disable certain rules. You can do this by selecting the rule's check box and clicking **Enable** or **Disable** as appropriate. Any disabled rules still appear in the search rules list but are ignored by the Cisco VCS when processing search requests.

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

You can test whether the Cisco VCS can find an endpoint identified by a given alias, without actually placing a call to that endpoint by using the Locate tool.

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

Filter queries to a zone without transforming

It is possible to 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 Cisco VCS to query the Sales Office Cisco 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 Cisco 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 Cisco VCS will not apply any further (lower priority) search rules.

To achieve the example described above, on your Head Office Cisco VCS create a zone to represent the Sales Office Cisco VCS, and from the **Create search rule** page (**VCS configuration > Dial plan > Search rules > New**) set up an associated search rule as follows:

Field	Value
Rule name	Regional sales office
Description	Calls to aliases with a suffix of @sales.example.com
Priority	100
Source	Any
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Suffix
Pattern string	@sales.example.com
Pattern behavior	Leave
On successful match	Stop
Target	Sales office
State	Enabled

Always query a zone with original alias (no transforms)

To configure a zone so that it is always sent search requests using the original alias, from the **Create search rule** page (**VCS 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

Field	Value
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: 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 Cisco VCS queries the zone for **name@example.co.uk** instead.

To achieve this, from the **Create search rule** page (**VCS 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 Cisco VCS from the **Create search rule** page (**VCS 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

Field	Value
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 a different replacement patterns. In this situation, the Cisco 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 Cisco VCS queries the zone simultaneously for both **name@example.co.uk** and **name@example.net**.

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

Rule #1

Field	Value
Rule name	Transform to example.co.uk
Description	Transform example.com to example.co.uk
Priority	100
Source	Any
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Suffix
Pattern string	example.com
Pattern behavior	Replace
Replace string	example.co.uk
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 Cisco 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 E164 number only.

Pre-search transform

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

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

Field	Value
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 (**VCS 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

Field	Value
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Regex
Pattern string	(\d+)@domain
Pattern behavior	Leave
On successful match	Continue
Target zone	Local Zone
State	Enabled

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

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

Transforms for alphanumeric H.323 ID dial strings

This example builds on the Stripping @domain for dialing to H.323 numbers 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 (**VCS 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 (**VCS 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

Field	Value
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 (**VCS 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

Configuring policy services

The **Policy services** page (**VCS configuration > Dial plan > Policy services**) is used to configure the external policy services that can be used as a target of the Cisco VCS's search rules.

The page lists all the currently configured policy services and lets you create, edit and delete services. Up to 5 policy services can be configured.

The configurable options are:

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 Cisco VCS automatically supports HTTP to HTTPS redirection when communicating with the policy service server.
Certificate verification mode	Controls whether the certificate presented by the policy service is verified when connecting over HTTPS.	When enabled, the value specified in the **Server address** field must be contained within the server's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes).
HTTPS certificate revocation list (CRL) checking	Controls certificate revocation list checking of the certificate supplied by the policy service. When enabled, the server's X.509 certificate is checked against the HTTPS certificate revocation list.	CRL data is uploaded to the Cisco VCS via the **HTTPS certificate revocation list** file on the Security certificates page.
Server address 1 - 3	The IP address or Fully Qualified Domain Name (FQDN) of the service.	For resiliency, up to three server addresses can be supplied.
Path	The URL of the service.	
Username	The username used by the Cisco VCS to log in and query the service.	
Password	The password used by the Cisco VCS to log in and query the service. The maximum plaintext length is 30 characters (which is subsequently encrypted).	
Default CPL	The default CPL used by the Cisco VCS if the policy service is unavailable.	This defaults to **<reject status='403' reason='Service Unavailable'/>** but you could change it, for example, to redirect to an answer service or recorded message.

About Call Policy

The Cisco VCS lets you 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 Cisco 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 Cisco VCS.

You should:

- use Call Policy to determine which callers can make or receive calls via the Cisco VCS
- use Registration restriction policy to determine which aliases can or cannot register with the Cisco VCS

Configuring Call Policy

The **Call Policy configuration** page (**VCS configuration > Call Policy> Configuration**) is used to configure the Cisco VCS's Call Policy mode and to upload local policy files.

Call Policy mode

The **Call Policy mode** controls from where the Cisco VCS obtains its Call Policy configuration. The options are:

- *Local CPL*: uses locally-defined Call Policy.
- *Directory and local CPL*: applies Call Policy defined in the directory service followed by any 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 Cisco VCS. If you choose *Local CPL* you must then either:

- upload a Call Policy file (containing CPL script), or
- configure basic Call Policy through the **Call Policy rules** page (**VCS configuration > Call Policy > Rules**). Note that this only lets you allow or reject specified calls.

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.

Directory and local CPL

The *Directory and local CPL* option refers Call Policy decisions, in the first instance, to the Directory service. This could be used, for example to determine if certain groups of users are allowed to call other groups of users.

If the directory service allows the call, any locally-defined Call Policy is then also applied. This enables you to apply further controls in addition to those provided by the directory service. For example, you can use local CPL to apply restrictions based on the source of incoming requests, or whether a request is authenticated or not.

Policy service

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 policy service:

Field	Description	Usage tips
Protocol	The protocol used to connect to the policy service.	The Cisco VCS automatically supports HTTP to HTTPS redirection when communicating with the policy service server.
Certificate verification mode	Controls whether the certificate presented by the policy service is verified when connecting over HTTPS.	When enabled, the value specified in the **Server address** field must be contained within the server's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes).
HTTPS certificate revocation list (CRL) checking	Controls certificate revocation list checking of the certificate supplied by the policy service. When enabled, the server's X.509 certificate is checked against the HTTPS certificate revocation list.	CRL data is uploaded to the Cisco VCS via the **HTTPS certificate revocation list** file on the Security certificates page.
Server address 1 - 3	The IP address or Fully Qualified Domain Name (FQDN) of the service.	For resiliency, up to three server addresses can be supplied.
Path	The URL of the service.	
Username	The username used by the Cisco VCS to log in and query the service.	
Password	The password used by the Cisco VCS to log in and query the service. The maximum plaintext length is 30 characters (which is subsequently encrypted).	
Default CPL	The default CPL used by the Cisco VCS if the policy service is unavailable.	This defaults to **<reject status='403' reason='Service Unavailable'/>** but you could change it, for example, to redirect to an answer service or recorded message.

Configuring Call Policy rules using the web interface

The **Call Policy rules** page (**VCS 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.

Note: 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 (**VCS configuration > Call Policy > Configuration**) you will have the option to **Delete uploaded file**. Doing so will delete the existing Call Policy that was put in place using a CPL script, and enable use of the **Call Policy rules** page for Call Policy configuration.

Each rule specifies the **Action** to take for all calls from a particular **Source** alias to a particular **Destination** alias. If you have more than one rule, you can **Rearrange** the order of priority in which these rules are applied.

The configurable options are:

Field	Description	Usage tips
Source pattern	The alias that the calling endpoint used to identify itself when placing the call. If this field is blank, the policy rule applies to all incoming calls from unauthenticated users, meaning calls where the endpoint making the call is **not** either: ▪ locally registered and authenticated with the Cisco VCS, or ▪ registered and authenticated to a neighbor which in turn has authenticated with the local Cisco VCS	See the Call Policy and authentication section for more information about unauthenticated users and Call Policy. This field supports regular expressions.
Destination pattern	The alias that the endpoint dialed to make the call.	This field supports regular expressions.
Action	Whether or not a call that matches the source and destination is permitted. *Allow*: if both the **Source** and **Destination** aliases match those listed, call processing will continue. *Reject*: if both the **Source** and **Destination** aliases match those listed, the call will be rejected.	
Rearrange	Each combination of **Source** and **Destination** is compared, in the order shown on the **Call Policy rules** page, with the details of the call being made until a match is found, at which point the call policy is applied. To move a particular item to higher or lower in the list, thus giving the rule a higher or lower priority, click on the and icons respectively.	

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

Configuring Call Policy using a CPL script

You can use CPL scripts to configure advanced Call Policy. To do this, you must first create and save the CPL script as a text file, after which you upload it to the Cisco VCS.

For information on the CPL syntax and commands that are supported by the Cisco VCS, see the CPL reference section.

Viewing existing CPL script

To view the Call Policy that is currently in place as an XML-based CPL script, go to the Call Policy configuration page (**VCS configuration > Call Policy > Configuration**) and click **Show Call Policy file**.

- If Call Policy has been configured using a CPL script, this shows you the script that was uploaded.
- If Call Policy has been configured using the **Call Policy rules** page, this shows you the CPL version of the 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 Cisco VCS without editing it, the Cisco 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 Cisco VCS. The **Call Policy configuration** page allows you to download the XML schemas which are used to check scripts that are uploaded to the Cisco 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 Cisco VCS.

Uploading a CPL script

To upload a new CPL file:

1. Go to the **Call Policy configuration** page (**VCS configuration > Call Policy > Configuration**). The CPL script cannot be uploaded using the command line interface.
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**.

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 Cisco VCS to use the Cisco TelePresence Advanced Media Gateway

The **Advanced Media Gateway configuration** page (**VCS configuration > Advanced Media Gateway > Configuration**) is used to configure how a Cisco VCS Control routes calls to or from a

Microsoft Office Communications Server (OCS) zone via the Cisco TelePresence Advanced Media Gateway (Cisco AM GW).

The Cisco AM GW provides support for transcoding between standard codecs (such as H.264) and Microsoft RT Video to allow high definition calls between Microsoft Office Communicator (MOC) clients and Cisco endpoints.

Configuring the Cisco VCS Control

For a Cisco VCS Control to use the Cisco AM GW you must first configure at least two zones:

- An OCS zone (a zone with a **Zone profile** set to *Microsoft Office Communications Server 2007*).
- A Cisco AM GW zone (a zone with a **Zone profile** set to *Cisco Advanced Media Gateway*). Note that a Cisco AM GW zone can be configured with up to six Cisco AM GW peers for load balancing purposes. Also note that Cisco AM GW zones do not require any associated search rules.

To start using the Cisco AM GW to transcode calls:

1. Go to the **Advanced Media Gateway configuration** page.
2. Click on the **Advanced Media Gateway zone** drop-down and choose the required Cisco AM GW zone. Note that only zones configured with a **Zone profile** of *Cisco Advanced Media Gateway* appear in this list.
   After a zone is selected, calls to or from the OCS are routed via the Cisco AM GWs connected to that zone.

By default, all OCS calls are routed via the Cisco AM GW.

If you want to control which calls go through the Cisco AM GW you have to set up policy rules. To do this, set **Policy mode** to *On* and then go to the Advanced Media Gateway policy rules page.

Usage features and limitations

- If the Cisco AM GW reaches its capacity, any calls that would normally route via the Cisco AM GW will not fail; the call will still connect as usual but will not be transcoded.
- The OCS zone must be inside any firewall; the endpoint receiving or making the call can be outside the firewall.
- The Cisco VCS shows calls routed via the Cisco AM GW as two calls: one from the endpoint via the Cisco VCS to the Cisco AM GW which will be a local or traversal call as appropriate, and then a separate call back from the Cisco AM GW via the Cisco VCS to the OCS which will always be a local call.
- Bandwidth controls can be applied to the leg of the call between the endpoint and the Cisco AM GW zone, but cannot be applied to the Cisco AM GW zone to OCS zone leg of the call.

For more information about configuring Cisco VCS, OCS and the Cisco AM GW, refer to the *Microsoft OCS 2007, Cisco VCS Control and Cisco AM GW* deployment guide [37].

Configuring Cisco AM GW policy rules

The **Advanced Media Gateway policy rules** page (**VCS configuration > Advanced Media Gateway > Policy rules**) lists the set of rules that control which calls can go through the Cisco AM GW.

By default, after a Cisco VCS Control has been configured with the Cisco AM GW to use for OCS calls, all calls to or from the OCS zone are routed via the Cisco AM GW.

The rules on this page are only applied if the **Policy mode** on the Advanced Media Gateway configuration page is set to *On*.

A rule is applied if it matches either the source or destination alias of a call. Note that if the aliases associated with a call do not match any of the policy rules, the call will be routed via the Cisco AM GW.

The page lists all the currently configured rules and lets you create, edit, delete, enable and disable rules. Note that you can click on a column heading to sort the list, for example by **Rule name** or **Priority**.

The configurable options are:

Field	Description	Usage tips
Rule 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.	
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 Cisco AM GW. *Deny*: the call can connect but it will not use Cisco AM GW resources.	

Field	Description	Usage tips
State	Indicates if the rule is enabled or not.	When you are making or testing configuration changes to your Cisco AM GW policy rules, you may want to temporarily enable or disable certain rules. You may also want to configure certain rules but only apply them occasionally. You can do this by selecting the rule's check box and clicking **Enable** or **Disable** as appropriate. Any disabled rules still appear in the rules list but are ignored by the Cisco VCS when determining which calls are routed via the Cisco AM GW.

Dialable 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 Cisco VCS follows when attempting to locate the destination endpoint. The address formats supported by the Cisco 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 Cisco 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 Cisco VCS, gatekeeper or Border Controller). See the IP dialing section for more information.

Endpoints registered to a Cisco VCS Expressway

Calls made by dialing the IP address of an H.323 endpoint registered directly with a Cisco VCS Expressway are forced to route through the Cisco 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 Cisco 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: 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 Cisco 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 Cisco VCS with at least one DNS server and at least one DNS zone.

Full instructions on how to configure the Cisco 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 Cisco VCS you must configure it with at least one DNS server and the appropriate ENUM zones.

Full instructions on how to configure the Cisco VCS to support ENUM dialing (both outbound and inbound) are given in the ENUM dialing section.

IP dialing

Dialing by IP address is necessary when the destination endpoint is not registered with any system (such as a Cisco VCS, Gatekeeper or Border Controller).

If the destination endpoint is registered with one of these systems, 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 via their IP addresses.

Calls to unknown IP addresses

Although the Cisco VCS supports dialing by IP address, it is sometimes undesirable for a Cisco VCS to be allowed to place a call directly to an IP address that is not local. Instead, you may want a neighbor to place the call on behalf of the Cisco VCS, or not allow such calls at all. The **Calls to unknown IP addresses** setting (on the **Dial plan configuration** page) configures how the Cisco VCS handles calls made to IP addresses which are not on its local network, or registered with it or one of its neighbors.

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

- is the IP address of a locally registered endpoint
- falls within the IP address range of one of the subzone membership rules configured on the Cisco VCS

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

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

- *Direct*: the Cisco VCS attempts to place the call directly to the unknown IP address without querying any neighbors.
- *Indirect*: the Cisco 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 Cisco VCS will pass the call to that neighbor for completion.
- *Off*: the Cisco VCS will not attempt to place the call, either directly or to any of its neighbors.

This setting applies to the call's destination address prior to any zone transforms, but after any pre-search transforms, Call Policy or User Policy rules have been applied.

Note that in addition to controlling calls, this setting also determines the behavior of provisioning 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:

- by dialing its URI (this requires that the local Cisco VCS is configured to support URI dialing, and a DNS record exists for that URI that resolves to the unregistered endpoint's IP address)
- by dialing its IP address

Recommended configuration for firewall traversal

When a Cisco VCS Expressway is neighbored with a Cisco VCS Control for firewall traversal, you should typically set **Calls to unknown IP addresses** to *Indirect* on the Cisco VCS Control and *Direct* on the Cisco 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 will go from the endpoint to the Cisco VCS Control with which it is registered.
2. As the IP address being called is not registered to that Cisco VCS, and its **Calls to unknown IP addresses** setting is *Indirect*, the Cisco VCS will not place the call directly. Instead, it will query its neighbor Cisco VCS Expressway to see if that system is able to place the call on the Cisco VCS Control's behalf.
3. The Cisco 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 Cisco VCS, calls to endpoints that are not registered locally or to a neighbor system could still be placed if the local Cisco VCS is neighbored (either directly or indirectly) with another Cisco 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 Cisco 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 Cisco VCS will query its local zone and neighbors for that URI.

If the Cisco 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 either:

- the H.323 endpoints should register with the Cisco 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 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 via 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 Cisco 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 section for more information.

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

Outgoing calls

To enable your Cisco 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 section.

Incoming calls

To enable endpoints registered to your Cisco 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 section.

Firewall traversal calls

To configure your system so that you can place and receive calls using URI dialing through a firewall, see the URI dialing and firewall traversal section.

URI resolution process using DNS

When a Cisco VCS is attempting to locate a destination URI address using the DNS system, the general process is as follows:

H.323

1. The Cisco 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 Cisco VCS, the query will be sent to all servers at the same time, and all responses will be prioritized by the Cisco 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 Cisco VCS will send an A/AAAA record query for each name record returned. These will resolve to one or more IP addresses, and the Cisco 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 Cisco VCS will send an A/AAAA record query for each name record returned. These will resolve to one or more IP addresses, and the Cisco 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 Cisco 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 Cisco VCS will not query for A and AAAA records and instead will continue with the search, querying the remaining lower priority zones.

SIP

The Cisco VCS supports the SIP resolution process as outlined in *RFC 3263* [16]. An example of how the Cisco VCS implements this process is as follows:

1. The Cisco 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 Cisco 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 Cisco VCS sends SRV queries for each result returned from the NAPTR record lookup. A prioritized list of A/AAAA records returned is built.
- The Cisco 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 Cisco 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 Cisco 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 Cisco VCS, or received as a query from a neighbor system:

1. The Cisco 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 Cisco VCS attempts to locate the endpoint through a DNS lookup. It does this by querying the DNS server configured on the Cisco 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 the **Zones** page (**VCS configuration > 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 Cisco 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 Cisco 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 Cisco 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 Cisco VCS to use DNS to locate endpoints outside your network, you must:

- configure the DNS servers used by the Cisco 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 Cisco VCS to receive incoming calls made using URI dialing via DNS relies on the presence of DNS records for each domain the Cisco VCS is hosting.

These records can be of various types including:

- A records, which provide the IPv4 address of the Cisco VCS
- AAAA records, which provide the IPv6 address of the Cisco VCS
- Service (SRV) records, which specify the FQDN of the Cisco 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 Cisco VCS.

Incoming call process

When an incoming call has been placed using URI dialing via DNS, the Cisco VCS will have been located by the calling system using one of the DNS record lookups described above. The Cisco 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 Cisco 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* [3] as:

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

For the Cisco 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 Cisco VCS is hosting (such as **example.com**)
- **Port** is the IP port on the Cisco VCS that has been configured to listen for that particular service and protocol combination
- **Target** is the FQDN of the Cisco VCS.

Configuring H.323 SRV records

Annex O of *H.323 specification* [15] 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 Cisco VCS supports two types of SRV record as defined by this Annex. These are Location and Call, with **_Service** set to **_h323ls** and **_h323cs** respectively.

If you want the Cisco VCS to be contactable using H.323 URI dialing, you should provide at least a Location SRV record, as it provides the most flexibility and the simplest configuration.

Location SRV records

For each domain hosted by the Cisco VCS, you should configure a Location SRV record as follows:

- **_Service** is **_h323ls**
- **_Proto** is **_udp**
- Port is the port number that has been configured from **VCS configuration > Protocols > H.323** as the **Registration UDP port**

Call SRV records

Call SRV records (and A/AAAA records) are intended primarily for use by endpoints which cannot participate in a location transaction, exchanging LRQ and LCF. The configuration of a Call SRV record should be as follows:

- **_Service** is **_h323cs**
- **_Proto** is **_tcp**
- Port is the port number that has been configured from **VCS configuration > Protocols > H.323** as the **Call signaling TCP port**.

Configuring SIP SRV records

RFC 3263 [16] 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 Cisco VCS to be contactable using SIP URI dialing, you should configure an SRV record for each SIP transport protocol enabled on the Cisco VCS (that is, UDP, TCP or TLS) as follows:

- Valid combinations of **_Service** and **_Proto** are:
  - **_sips._tcp**
  - **_sip._tcp**
  - **_sip._udp**
- Port is the IP port number that has been configured from **VCS configuration > Protocols > SIP** as the port for that particular transport protocol.

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 Cisco 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**
- NAPTR record for **example.com** returns
  - **_sip._tcp.example.com** and
  - **_sip._udp.example.com** and
  - **_sips._tcp.example.com**
- SRV record for **_sip._udp.example.com** returns **vcs.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 Cisco VCS
- AAAA record for **vcs.example.com** returns the IPv6 address of the Cisco 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 section.

For locally registered H.323 endpoints to be reached using URI dialing, either:

- the H.323 endpoints should register with the Cisco 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 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 Cisco 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 Cisco VCS Expressway and any Cisco VCSs on the public network only. Cisco 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 Cisco VCS will be routed through the Cisco VCS Expressway.

In addition, the DNS records for incoming calls should be configured with the address of the Cisco VCS Expressway as the authoritative gatekeeper/proxy for the enterprise (the DNS configuration examples section for more information). This ensures that incoming calls placed using URI dialing enter the enterprise through the Cisco 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 Cisco 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 Cisco VCS supports outward ENUM dialing by allowing you to configure ENUM zones on the Cisco VCS. When an ENUM zone is queried, this triggers the Cisco 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 a Cisco VCS is attempting 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 Cisco 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 Cisco 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 locally registered endpoints to dial out to other endpoints using ENUM, you must:

- configure at least one ENUM zone, and
- configure at least one DNS Server

This is described in the ENUM dialing for outgoing calls section.

Incoming Calls

To enable endpoints in your enterprise to receive incoming calls from other endpoints via ENUM dialing, you must configure a DNS NAPTR record mapping your endpoints' E.164 numbers to their SIP/H.323 URIs. See the ENUM dialing for incoming calls section for instructions on how to do this.

Note: if an ENUM zone and a DNS server have not been configured on the local Cisco VCS, calls made using ENUM dialing could still be placed if the local Cisco VCS is neighbored with another Cisco 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

Prerequisites

For a local endpoint to be able to dial another endpoint using ENUM via your Cisco 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 Cisco 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 Cisco 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 process below is followed when an ENUM (E.164) number is dialed from an endpoint registered with your Cisco VCS:

1. The user dials the E.164 number from their endpoint.
2. The Cisco VCS initiates a search for the E.164 number as dialed. It follows the usual call routing process.

3. After applying any pre-search transforms, the Cisco 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
4. 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 Cisco VCS attempts to locate the endpoint through ENUM. As and when each ENUM zone configured on the Cisco VCS is queried, the E.164 number is transformed into an ENUM domain as follows:
     i. The digits are reversed and separated by a dot.
     ii. The **DNS suffix** configured for that ENUM zone is appended.
5. DNS is then queried for the resulting ENUM domain.
6. 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 Cisco VCS.
7. The Cisco VCS then initiates a new search for that URI (maintaining the existing hop count). The Cisco 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 Cisco 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 Cisco 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 Cisco 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 Cisco VCS that the E.164 number we have dialed is mapped to the SIP URI of **fred@example.com**.
8. The Cisco 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.

Zone configuration for ENUM dialing

For locally registered endpoints to use 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 the **Zones** page (**VCS configuration > 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 Cisco 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 Cisco 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 Cisco VCS with details of DNS servers to be used when searching for NAPTR records.

Configuring matches for ENUM zones

If you want locally registered endpoints to be able to make ENUM calls via the Cisco 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 Cisco VCS, and then an associated search rule with:

- **Mode** of *Alias pattern match*
- **Pattern string** of **44**
- **Pattern type** of *Prefix*

This will result 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 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 Cisco 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 SIP/H.323 URIs. This record must be located at an appropriate DNS domain where it can be found by any systems attempting to reach you by using ENUM dialing.

About DNS domains for ENUM

ENUM relies on the presence of NAPTR records to provide the mapping between E.164 numbers and their SIP/H.323 URIs.

RFC 3761 [8], 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 [7]. These are used to obtain an H.323 or SIP URI from an E.164 number.

The record format that the Cisco VCS supports is:

order flag preference service regex replacement

where:

- **order** and **preference** determine the order in which NAPTR records are processed. The record with the lowest order is processed first, with those with the lowest preference being processed first in the case of matching order.
- **flag** determines the interpretation of the other fields in this record. Only the value **u** (indicating that this is a terminal rule) is currently supported, and this is mandatory.

- **service** states whether this record is intended to describe E.164 to URI conversion for H.323 or for SIP. Its value must be either **E2U+h323** or **E2U+SIP**.
- **regex** is a regular expression that describes the conversion from the given E.164 number to an H.323 or SIP URI.
- **replacement** is not currently used by the Cisco VCS and should be set to . (the full stop character).

Non-terminal rules in ENUM are not currently supported by the Cisco VCS. For more information on these, see section 2.4.1 of RFC 3761 [8],

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 Cisco 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 Cisco VCS will query when attempting to locate a domain. These fields must use an IP address, not a FQDN.

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.

Call signaling configuration

The **Calls** page (**VCS configuration > Calls**) is used to configure the Cisco VCS's call signaling functionality.

Call routed mode

Calls are made up of two components - signaling and media. For traversal calls, the Cisco VCS always handles both the media and the signaling. For non-traversal calls, the Cisco VCS does not handle the media, and may or may not need to handle the signaling.

The **Call routed mode** setting specifies whether the Cisco VCS removes itself, where it can, from the call signaling path after the call has been set up. The options for this setting are:

- *Always*: the Cisco VCS always handles the call signaling. The call consumes either a traversal call license (if it is a traversal call) or a local (non-traversal) call license (if it is not a traversal call) on the Cisco VCS.
- *Optimal*: the Cisco 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 it resolves to more than one alias, or has a "no answer" or "busy" device configured
  - one of the endpoints in the call is locally registered

  In all other cases the Cisco VCS removes itself from the call signaling path after the call has been set up. The Cisco 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 central Cisco VCS. In such deployments the central Cisco 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 Cisco VCS can be configured to detect search loops within your network and terminate such searches through the **Call loop detection mode** setting. The options for this setting are:

- *On*: the Cisco 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:
  - have same call tag
  - are for the same destination alias
  - use the same protocol, and
  - originate from the same zone

  Using this setting allows you to save on network resources and fail call branches early where loops have been detected.
- *Off*: the Cisco VCS will not detect and fail search loops. You are recommended to use this setting only in advanced deployments.

Note: the loop detection feature was introduced in Cisco VCS version X4. It is only supported in deployments where all Cisco VCSs are running on X4 software or later.

Identifying calls

Each call that passes through the Cisco 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 Cisco 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 Cisco 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 Cisco VCS web interface does not show the Call ID.

Call Serial Number

The Cisco VCS assigns a unique Call Serial Number to every call passing through it. No two calls on a Cisco VCS will ever have the same Call Serial Number. A single call passing between two or more Cisco 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 Cisco VCSs. When the Cisco VCS receives a call, it checks to see if there is a Call Tag already assigned to it. If so, the Cisco 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 Cisco VCSs will be assigned a different Call Serial Number each time it arrives at a Cisco 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 Cisco 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 Cisco 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.

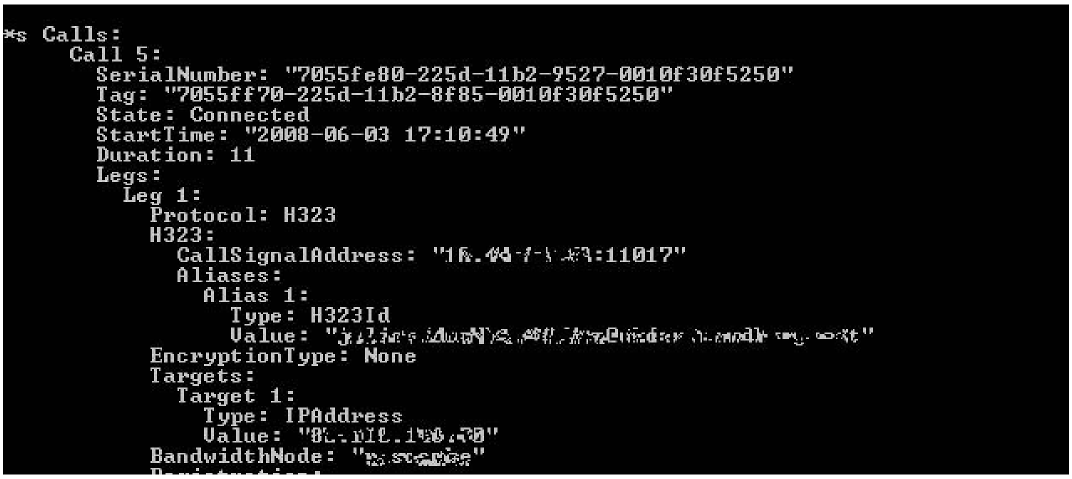
Note: Call Tags are supported by Cisco VCS version X3.0 or later. If a call passes through a system that is not a Cisco VCS, or a Cisco VCS that is running an earlier version of the software, the Call Tag information will be lost.

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, for example:



```
*s Calls:
    Call 5:
      SerialNumber: "7055fe80-225d-11b2-9527-0010f30f5250"
      Tag: "7055ff70-225d-11b2-8f85-0010f30f5250"
      State: Connected
      StartTime: "2008-06-03 17:10:49"
      Duration: 11
      Legs:
        Leg 1:
          Protocol: H323
          H323:
            CallSignalAddress: "[redacted]:11017"
            Aliases:
              Alias 1:
                Type: H323Id
                Value: "[redacted]"
          EncryptionType: None
          Targets:
            Target 1:
              Type: IPAddress
              Value: "[redacted]"
          BandwidthNode: "[redacted]"
```

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 Cisco 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). 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 Cisco VCS also allows you to reference the call using the longer but unique call serial number.

Note: when disconnecting a call, only the call with that Call Serial Number is disconnected. Other calls with the same Call Tag but a different Call Serial Number may not be affected.

Limitations when disconnecting SIP calls

Call disconnection works differently for H.323 and SIP calls due to differences in the way the protocols work.

For H.323 calls, and interworked calls, the **Disconnect** command actually disconnects the call.

For SIP calls, the **Disconnect** command causes the Cisco VCS to release all resources used for the call; the call will appear as disconnected on the Cisco VCS. SIP calls are peer-to-peer, and as the Cisco VCS is a SIP proxy it has no authority over the endpoints. Releasing the resources on the Cisco VCS may have the side-effect of disconnecting the SIP call, but 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 released their resources.

Note: endpoints that support SIP session timers (RFC 4028 [14]) have a call refresh timer which allows them to detect a hung call (signaling lost between endpoints). The endpoints can then release their resources after the negotiated timeout period.

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 (**VCS configuration > Local Zone** and **VCS configuration > Bandwidth**).

It includes the following information:

- an overview of bandwidth control and subzones
- how to configure subzones and membership rules
- how to configure links and pipes
- some bandwidth control examples

About bandwidth control

The Cisco 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.

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 command **xCommand CheckBandwidth**.

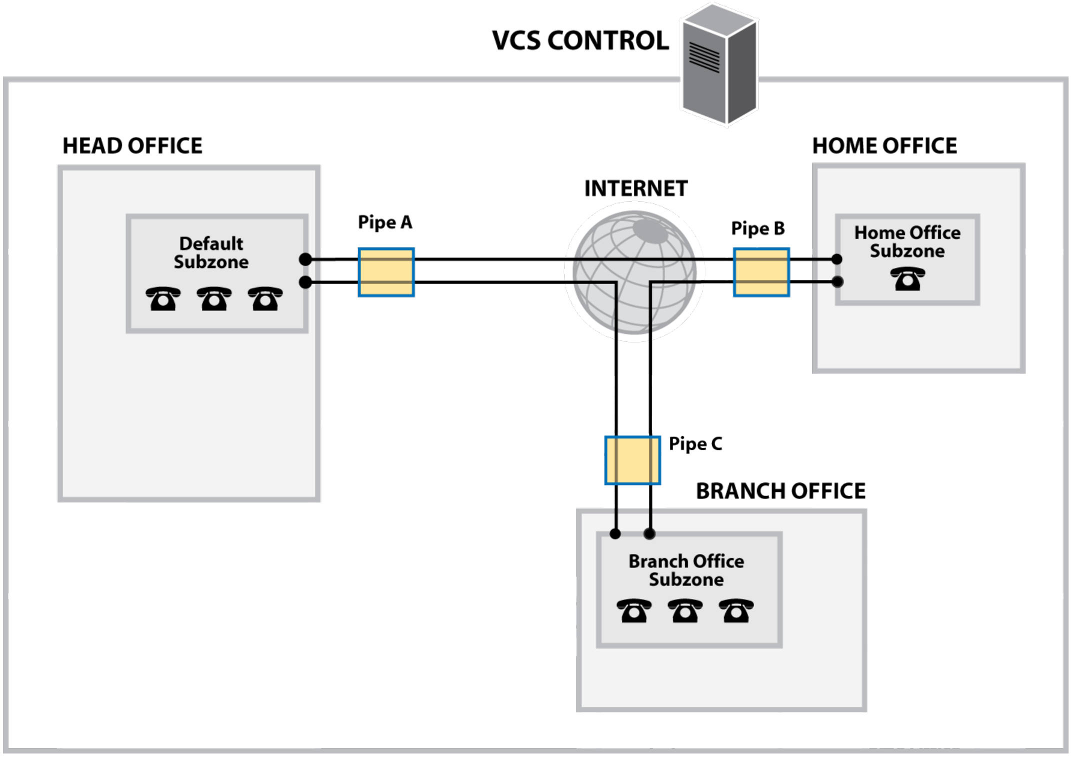
For specific information about how bandwidth is managed across peers in a cluster, see Sharing bandwidth across peers.

Example network deployment

The diagram below 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.



Bandwidth configuration

The **Bandwidth configuration** page (**VCS configuration > Bandwidth > Configuration**) is used to specify how the Cisco 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 options are:

Field	Description	Usage tips
Default call bandwidth (kbps)	The bandwidth value to be used for calls for which no bandwidth value has been specified by the system that initiated the call. 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.	

Field	Description	Usage tips
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 Cisco 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 registrations.

When an endpoint registers with the Cisco 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 (**VCS configuration > Local Zone > Subzones**).

Three special subzones — the Default Subzone, the Traversal Subzone and the Cluster Subzone (only applies if the Cisco VCS is in a cluster) — are automatically created and cannot be deleted.

Default links between subzones

The Cisco VCS is shipped with the Default Subzone and Traversal Subzone (and Default Zone) already created, and with links between the three. 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 (**VCS 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 are deemed to pass through the Traversal Subzone, so by applying bandwidth limitations to the Traversal Subzone you can control how much processing of media the Cisco 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 for more details.

Configuring the Traversal Subzone ports

The Cisco VCS allows you to configure the range of ports used for the media in traversal calls. A single traversal call can consist of up to 5 types of media (audio, video, far end camera control, dual streams and BFCP) and each type of media may require a pair of ports – for example, audio and video each require one port for RTP, and one for RTCP. Separate pairs of ports are required for the inbound and outbound portions of a call. A single traversal call can therefore take up to 20 ports.

The default range for the ports to be used for media is 50000 - 52399 UDP, but these can be changed to any values between 1024 and 65533. Ports are allocated from this range in pairs, with the first port number of each pair being an even number. Therefore the range must start with an even number and end with an odd number.

To configure the ports used for media in traversal calls, go to **VCS configuration > Local Zone > Traversal Subzone**.

Note: you must ensure that the port range is large enough to support the maximum number of traversal calls available on your Cisco VCS. A single traversal call can take up to 20 ports (5 pairs in each direction). So for example, if your Cisco VCS is licensed for 5 traversal calls you must ensure that the range of ports configured for traversal media is at least 100. If you add extra traversal calls to your system, you must also ensure that the range of ports available is sufficient.

About the Default Subzone

The **Default Subzone** page (**VCS 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 and authentication policies.

When an endpoint registers with the Cisco 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 configured 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.

Configuring subzones

The **Subzones** page (**VCS configuration > Local Zone > Subzones**) lists all the subzones that have been configured on the Cisco 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 Cisco VCS.

Subzone registration policy

When an endpoint registers with the Cisco 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 Cisco VCS, you can also configure each manually created subzone and the Default Subzone 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.

Subzone authentication policy

To control the services available to endpoints registered to a subzone you can specify how each subzone authenticates incoming messages and whether they are subsequently treated as authenticated, unauthenticated or are rejected.

See the Authentication Policy configuration options section for more information about the policy settings, and how they are applied to zones and subzones.

Bandwidth controls

When configuring your subzones you can apply bandwidth limits to:

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

See Applying bandwidth limitations to subzones for information about how the bandwidth limits are set and managed.

Configuring subzone membership rules

The **Subzone membership rules** page (**VCS 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 Cisco VCS.

The page lists all the subzone membership rules that have been configured on the Cisco VCS, and lets you create, edit, delete, enable and disable rules. Up to 3000 subzone membership rules can be configured.

Note: if the endpoint’s IP address or registration alias does not match any of the membership rules, it is assigned to the Default Subzone.

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*.
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.	

Enabling and disabling membership rules

When you are making or testing configuration changes to your membership rules, you may want to temporarily enable or disable certain rules. You can do this by selecting the rule's check box and clicking **Enable** or **Disable** as appropriate. Any disabled rules still appear in the membership rules list but are ignored by the Cisco VCS when processing registration requests.

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 both 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 128, 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 Cisco VCS will perform the bandwidth calculations using the one with the fewest links.

The **Links** page (**VCS 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 two subzones, or one subzone and one zone, that the link is between.
Pipe 1 and Pipe 2	Any pipes that have been used to apply bandwidth limitations to the link. See Applying pipes to links for more information.
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.

Whenever a subzone or zone is created, certain links are automatically created; see Default links for further information.

Default links

If a subzone has no links configured, then endpoints within the subzone will only be able to call other endpoints within the same subzone. For this reason, the Cisco 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 Cisco VCS is shipped with the Default Subzone, Traversal Subzone and Default Zone already created, and with default links pre-configured between the three which are named as follows: *DefaultSZtoTraversalSZ*, *DefaultSZtoDefaultZ* and *TraversalSZtoDefaultZ*.

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. To apply these limits, you must first create a pipe and configure it with the required bandwidth limitations. Then when configuring links you assign the pipe to one or more links. Calls using the link will then have the pipe's bandwidth limitations applied to them. See Applying pipes to links for more information.

The **Pipes** page (**VCS configuration > Bandwidth > Pipes**) lists all the pipes that have been configured on the Cisco 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 for 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 will restrict the bandwidth of calls made between the two nodes of the link - the restrictions will 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

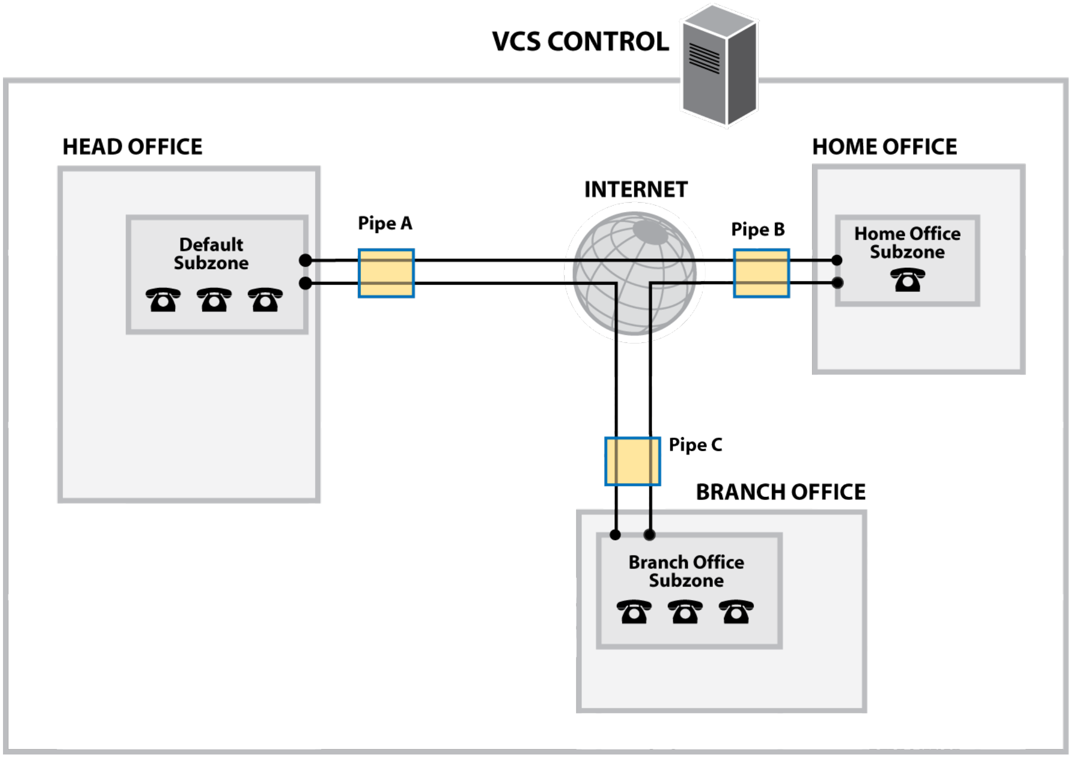
Each pipe may be applied to multiple links. This is used to model the situation where one site communicates with several other sites over the same broadband connection to the Internet. A pipe should be configured to represent the broadband connection, and then applied to all the links. This allows you 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

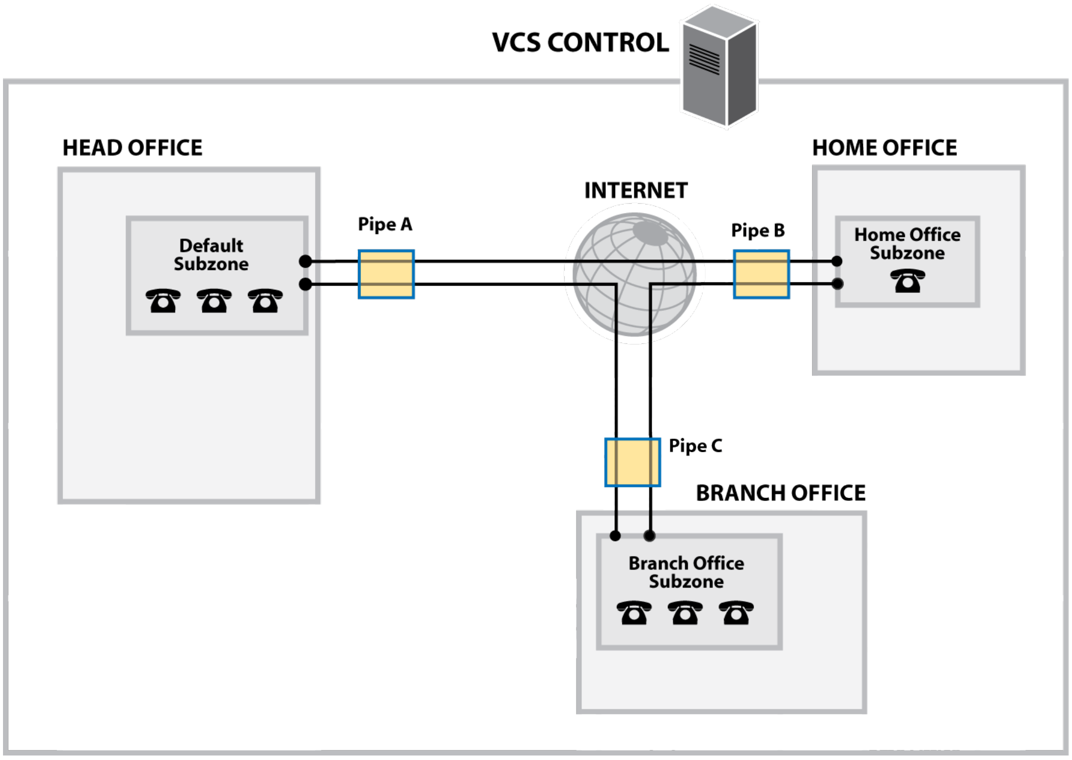
In the example below, there are three geographically separate offices: Head, Branch and Home. All endpoints in the Head Office register with the Cisco VCS Control, as do those in the Branch and Home offices.

Each of the three offices is represented as a separate subzone on the Cisco 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

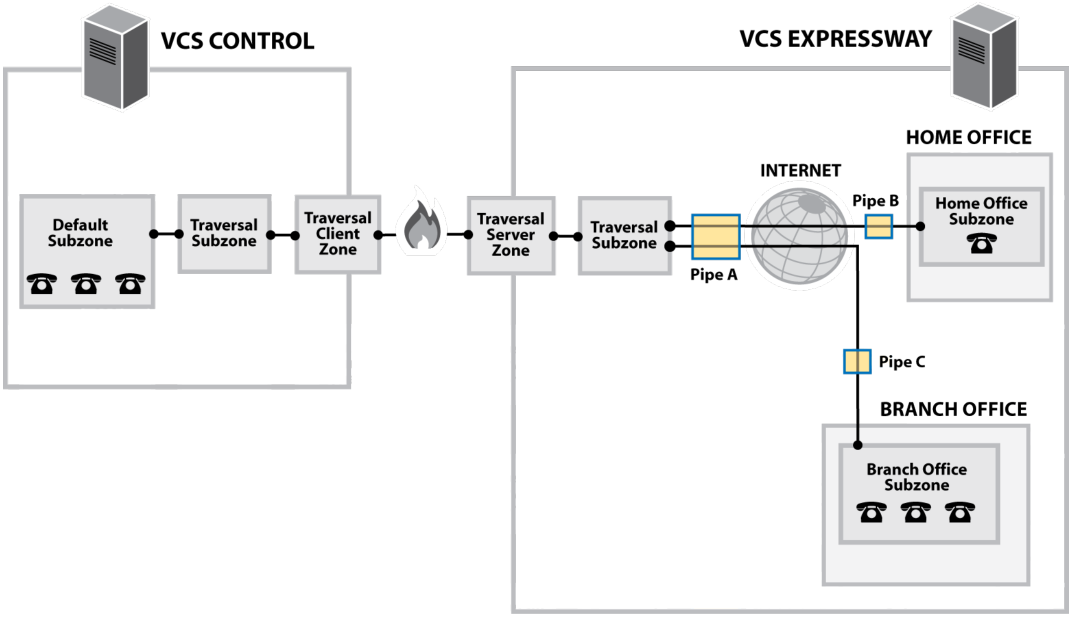
If the example deployment above is modified to include firewalls between the offices, we can use Cisco's Expressway firewall traversal solution to maintain connectivity. We do this by adding a Cisco VCS Expressway outside the firewall on the public internet, which will work in conjunction with the Cisco 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 Cisco VCS Control, while those in the Branch and Home offices register with the Cisco 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 Cisco VCS Expressway. This is shown by the absence of a link between the Home and Branch subzones.

The Cisco VCS Expressway has subzones configured for the Home Office and Branch Office. These are linked to the Cisco VCS Expressway's Traversal Subzone, with pipes placed on each link. All calls from the Cisco VCS Expressway to the Cisco 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 Cisco 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 Cisco 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.


VCS CONTROL
Default Subzone
Traversal Subzone
Traversal Client Zone
VCS EXPRESSWAY
Traversal Server Zone
Traversal Subzone
Pipe A
INTERNET
Pipe B
HOME OFFICE
Home Office Subzone
Pipe C
BRANCH OFFICE
Branch Office Subzone

Firewall traversal

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

It includes the following information:

- an overview of firewall traversal
- how to configure the Cisco VCS as a traversal client and as a traversal server
- firewall traversal protocols and ports
- firewall configuration guidelines
- an overview of ICE and TURN services

About firewall traversal

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

Expressway solution

The Expressway solution consists of:

- a Cisco VCS Expressway or Border Controller located outside the firewall on the public network or in the DMZ, which acts as the firewall traversal server
- a Cisco VCS Control, Gatekeeper, MXP endpoint or other traversal-enabled endpoint located in a private network, which acts as the firewall traversal client

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

How does it work?

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

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

For firewall traversal to function correctly, the Cisco 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 Cisco VCS Expressway; the settings for these connections are configured in a different way). Likewise, each Cisco 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 Quick guide to Cisco VCS traversal client - server configuration for a summary of the required configuration on each system. Because the Cisco VCS Expressway listens for connections from the client on a specific port, you are recommended to create the traversal server zone on the Cisco VCS Expressway before you create the traversal client zone on the Cisco VCS Control.

Cisco VCS as a firewall traversal client

Your Cisco VCS can act as a firewall traversal client on behalf of SIP and H.323 endpoints registered to it, and any gatekeepers that are neighbored with it. To act as a firewall traversal client, the Cisco VCS must be configured with information about the systems that will act as its firewall traversal server.

You do this by adding a new traversal client zone on the Cisco VCS client (**VCS configuration > Zones**) and configuring it with the details of the traversal server. See Configuring traversal client zones for more information. You can create more than one traversal client zone if you want to connect to multiple traversal servers.

Note that:

- In most cases, you will use a Cisco VCS Control as a firewall traversal client. However, a Cisco VCS Expressway can also act as a firewall traversal client.
- The firewall traversal server used by the Cisco VCS client can be a Cisco VCS Expressway, or (for H.323 only) a TANDBERG Border Controller.

Cisco VCS as a firewall traversal server

The Cisco VCS Expressway has all the functionality of a Cisco 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 Cisco VCS Expressway to act as a firewall traversal server for Cisco systems, you must create and configure a traversal server zone on the Cisco VCS Expressway (**VCS configuration > Zones**) and configure it with the details of the traversal client. See Configuring traversal server zones for more information.

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

Configuring other traversal server features

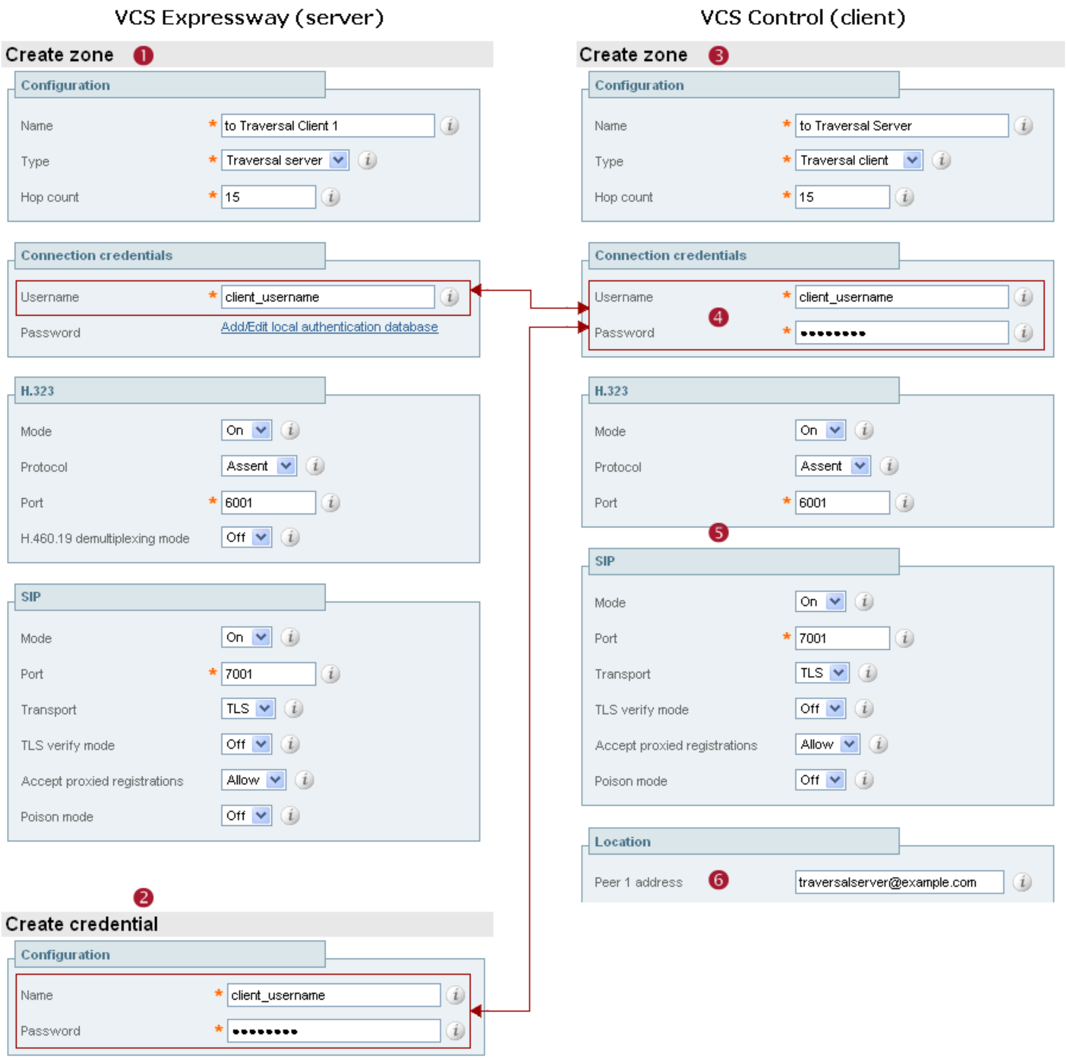
- For the Cisco VCS Expressway to act as a firewall traversal server for traversal-enabled endpoints (such as Cisco MXP endpoints and any other endpoints that support the ITU H.460.18 and H.460.19 standards), no additional configuration is required. See Configuring traversal for endpoints for more information.
- To enable TURN relay services and find out more about ICE, see About ICE and TURN services.
- To reconfigure the default ports used by the Cisco VCS Expressway, see Configuring traversal server ports.

Quick guide to Cisco VCS traversal client - server configuration

Full details of how to configure a Cisco VCS Control and Cisco VCS Expressway as traversal client and server respectively are given in the following sections. However, the basic steps are as follows:

Step	Description
❶	On the Cisco VCS Expressway, create a traversal server zone (this represents the incoming connection from the Cisco VCS Control). In the **Username** field, enter the Cisco VCS Control’s authentication username.

Step	Description
2	On the Cisco VCS Expressway, add the Cisco VCS Control’s authentication username and password as credentials into the local authentication database. Click the **Add/Edit local authentication database** link on the **Create zone** page to open the **Local authentication database** page from where you can add new credentials.
3	On the Cisco VCS Control, create a traversal client zone (this represents the connection to the Cisco VCS Expressway).
4	On the Cisco VCS Control, enter the same authentication **Username** and **Password** as specified on the Cisco 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 Cisco VCS Expressway.
6	Enter the Cisco VCS Expressway’s IP address or FQDN in the **Peer 1 address** field.



VCS Expressway (server)

Create zone 1

Configuration

Name *	to Traversal Client 1
Type *	Traversal server
Hop count *	15

Connection credentials

Username *	client_username
Password	Add/Edit local authentication database

H.323

Mode	On
Protocol	Assent
Port *	6001
H.460.19 demultiplexing mode	Off

SIP

Mode	On
Port *	7001
Transport	TLS
TLS verify mode	Off
Accept proxied registrations	Allow
Poison mode	Off

2

Create credential

Configuration

Name *	client_username
Password *	••••••••

VCS Control (client)

Create zone 3

Configuration

Name *	to Traversal Server
Type *	Traversal client
Hop count *	15

Connection credentials

4

Username *	client_username
Password *	••••••••

H.323

Mode	On
Protocol	Assent
Port *	6001

5

SIP

Mode	On
Port *	7001
Transport	TLS
TLS verify mode	Off
Accept proxied registrations	Allow
Poison mode	Off

Location

Peer 1 address 6	traversalserver@example.com

Firewall traversal protocols and ports

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

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

The Port usage pages (under **Maintenance > Tools > Port usage**) show, in table format, all the IP ports that are being used on the Cisco VCS, both inbound and outbound. This information can be provided to your firewall administrator so that the firewall can be configured appropriately.

Expressway process

The Expressway solution works as follows:

1. Each traversal client connects via the firewall to a unique port on the Cisco 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 has been established, the client constantly sends a probe to the Cisco VCS Expressway via this connection in order to keep the connection alive.
4. When the Cisco 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).

H.323 firewall traversal protocols

The Cisco 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 Cisco 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.

Ports for initial connections from traversal clients

Each traversal server zone specifies an **H.323 port** and a **SIP port** to be used for the initial connection from the client.

Each time you configure a new traversal server zone on the Cisco 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 Cisco VCS Expressway, matching ports must be configured on the corresponding traversal client.

Note:

- The default port used for the initial connections from MXP endpoints is the same as that used for standard RAS messages, that is UDP/1719. While it is possible to change this port on the Cisco VCS Expressway, most endpoints will not support connections to ports other than UDP/1719. You are therefore recommended to 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 Cisco VCS Expressway's traversal server zones.

Default port summary

The following table shows the default ports used for connections to the Cisco VCS Expressway.

Protocol	Call signaling	Media
Assent	UDP/1719: listening port for RAS messages TCP/2776: listening port for H.225 and H.245 protocols	UDP/2776: RTP media port UDP/2777: RTCP media control port
H.460.18/19	UDP/1719: listening port for RAS messages TCP/1720: listening port for H.225 protocol TCP/2777: listening port for H.245 protocol	UDP/2776: RTP media port UDP/2777: RTCP media control port UDP/50000-52399: demultiplex media port range
SIP	SIP call signaling uses the same port as used by the initial connection between the client and server.	Where the traversal client is a Cisco VCS, SIP media uses Assent to traverse the firewall. The default ports are the same as for H.323: UDP/2776: RTP media port UDP/2777: RTCP media control port

You have the option to change these ports if necessary by going to the Ports page (**VCS configuration > Expressway > Ports**).

If your Cisco 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 Cisco VCS Control and Cisco VCS Expressway.

TURN ports

The Cisco VCS Expressway can be enabled to provide TURN services (Traversal Using Relays around NAT) which can be used by SIP endpoints that support the ICE firewall traversal protocol.

The ports used by these services are configurable on the TURN page (**VCS configuration > Expressway > 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.

Ports for connections out to the public internet

In situations where the Cisco 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 Cisco VCS Expressway only after the server has located the endpoint on the public internet. This may cause problems if your Cisco VCS Expressway is located within a DMZ (that is, there is a firewall between the Cisco VCS Expressway and the public internet) as you will not be able to specify in advance rules that will allow you to connect out to the endpoint’s ports.

You can however specify the ports on the Cisco 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. The ports that can be configured for this purpose are:

H.323	SIP	TURN
TCP/1720: signaling UDP/1719: signaling UDP/50000-52399: media TCP/15000-19999: signaling	TCP/5061: signaling UDP/5060 (default): signaling UDP/50000-52399: media TCP: a temporary port in the range 25000-29999 is allocated	UDP/3478 (default): TURN services UDP/60000-61200 (default range): media

Firewall traversal and authentication

To control which systems can use the Cisco VCS Expressway as a traversal server, each Cisco VCS Control or Gatekeeper that wants to be its client must first authenticate with it.

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

The settings used for authentication depend on the combination of client and server being used. These are detailed in the table below.

Client	Server
Cisco VCS Control or Cisco VCS Expressway The Cisco VCS client provides its **Username** and **Password**. These are set on the traversal client zone by using **VCS configuration > Zones > Edit zone**, in the **Connection credentials** section.	**Cisco VCS Expressway** The traversal server zone for the Cisco VCS client must be configured with the client's authentication **Username**. This is set on the Cisco VCS Expressway by using **VCS configuration > Zones > Edit zone**, in the **Connection credentials** section. There must also be an entry in the Cisco VCS Expressway's authentication database with the corresponding client username and password.
Endpoint The endpoint client provides its **Authentication ID** and **Authentication Password**.	**Cisco VCS Expressway** There must be an entry in the Cisco VCS Expressway's authentication database with the corresponding client username and password.
TANDBERG Gatekeeper (version 5.2 and earlier) The Gatekeeper looks up its **System Name** in its own authentication database and retrieves the password for that name. It then provides this name and password.	**Cisco VCS Expressway** The traversal server zone for the Gatekeeper client must be configured with the Gatekeeper's **System Name** in the **Username** field. This is set on the Cisco VCS Expressway by using **VCS configuration > Zones > Edit zone**, in the **Connection credentials** section. There must be an entry in the Cisco VCS Expressway's authentication database that has the Gatekeeper's **System name** as the username, along with the corresponding password.
TANDBERG Gatekeeper (version 6.0 or later; 6.1 or later is recommended) The Gatekeeper provides its **Authentication Username** and **Authentication Password**. These are set on the Gatekeeper by using **Gatekeeper Configuration > Authentication**, in the **External Registration Credentials** section.	**Cisco VCS Expressway** The traversal server zone for the Gatekeeper client must be configured with the Gatekeeper's **Authentication Username** in the **Username** field. This is set on the Cisco VCS Expressway by using **VCS configuration > Zones > Edit zone**, in the **Connection credentials** section. There must also be an entry in the Cisco VCS Expressway's authentication database with the corresponding client username and password.

Client	Server
Cisco VCS Control or Cisco VCS Expressway If authentication is enabled on the Border Controller, the Cisco VCS client provides its **Username** and **Password**. These are set on the traversal client zone by using **VCS configuration > Zones > Edit zone**, in the **Connection credentials** section. If the Border Controller is in *Assent* mode, the Cisco VCS client provides its **Username**. This is set on the traversal client zone by using **VCS configuration > Zones > Edit zone**, in the **Connection credentials** section.	**TANDBERG Border Controller** If authentication is enabled on the Border Controller, there must be an entry in the Border Controller's authentication database that matches the Cisco VCS client's authentication **Username** and **Password**. If the Border Controller is in *Assent* mode, the traversal zone configured on the Border Controller to represent the Cisco VCS client must use the Cisco VCS's authentication **Username** in the Assent **Account name** field. This is set on the Border Controller via **TraversalZone > Assent > Account name**.

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

Authentication and NTP

All Cisco VCS and Gatekeeper traversal clients that support H.323 must authenticate with the Cisco VCS Expressway. The authentication process makes use of timestamps and requires that each system uses an accurate system time. The system time on a Cisco 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.

Firewall traversal and Dual Network Interfaces

The Dual Network Interfaces option key enables the LAN 2 interface on your Cisco VCS Expressway (the option is not available on a Cisco VCS Control). The LAN 2 interface is used in situations where your Cisco 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 Cisco VCS with two separate IP addresses, one for each network in the DMZ. Your Cisco 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.

Note: all ports configured on the Cisco VCS, including those relating to firewall traversal, apply to both IP addresses; it is not possible to configure these ports separately for each IP address.

Firewall configuration

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

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

Cisco offers a downloadable tool, the Expressway Port Tester, that allows you to test your firewall configuration for compatibility issues with your network and endpoints. It will advise if necessary which ports may need to be opened on your firewall in order for the Expressway™ solution to function correctly. The Expressway Port Tester currently only supports H.323. Contact your Cisco representative for more information.

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

The Port usage pages (under **Maintenance > Tools > Port usage**) show, in table format, all the IP ports that are being used on the Cisco VCS, both inbound and outbound. This information can be provided to your firewall administrator so that the firewall can be configured appropriately.

Configuring traversal for endpoints

Traversal-enabled H.323 endpoints can register directly with the Cisco VCS Expressway and use it for firewall traversal.

The **Locally registered endpoints** page (**VCS configuration > Expressway > Locally registered endpoints**) allows you to configure the way in which the Cisco 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.
H.460.19 demux mode	Determines whether the Cisco VCS Expressway operates in demultiplexing mode for calls from locally registered endpoints. *On*: allows use of the same two ports for all calls. *Off*: each call uses a separate pair of ports for media.
H.323 preference	Determines which protocol the Cisco 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 Cisco VCS Expressway.
UDP probe retry count	The number of times locally registered endpoints attempt to send a UDP probe to the Cisco VCS Expressway.
UDP probe keep alive interval	The interval (in seconds) with which locally registered endpoints send a UDP probe to the Cisco 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 Cisco VCS Expressway.
TCP probe retry count	The number of times locally registered endpoints attempt to send a TCP probe to the Cisco VCS Expressway.

Field	Description
TCP probe keep alive interval	The interval (in seconds) with which locally registered endpoints send a TCP probe to the Cisco VCS Expressway after a call is established, in order to keep the firewall's NAT bindings open.

Configuring traversal server ports

The Cisco 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 (**VCS configuration > Expressway > Ports**).

The options are:

Field	Description
Media demultiplexing RTP port	Port used for demultiplexing RTP media. Default is *2776*.
Media demultiplexing RTCP port	Port used for demultiplexing RTCP media. Default is *2777*.
H.323 Assent call signaling port	Port used for Assent signaling. Default is *2776*.
H.323 H.460.18 call signaling port	Port used for H.460.18 signaling. Default is *2777*.

See Firewall traversal protocols and ports for more information.

About ICE and TURN services

About ICE

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

It allows endpoints (clients) residing behind NAT devices to discover paths through which they can pass media, verify peer-to-peer connectivity via each of these paths and then select the optimum media connection path. The available paths typically depend on any inbound and outbound connection restrictions that have been configured on the NAT device. Such behavior is described in *RFC 4787* [13].

An example usage of ICE is two home workers communicating via the internet. If the two endpoints can communicate via ICE the Cisco 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 Cisco VCS also takes the media and thus requires a traversal licence.

For more information about ICE, refer to *RFC 5245* [38].

About TURN

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

For more information about TURN refer to *RFC 5766* [12], and for detailed information about the base STUN protocol, refer to *RFC 5389* [11].

TURN relay server

The Cisco VCS Expressway's TURN relay server can be configured to provide TURN services to traversal clients (see Configuring TURN services).

How TURN is used by an ICE client

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

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

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

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

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

Capabilities and limitations

- The Cisco VCS supports up to 1800 relay allocations. This is typically enough to support 100 calls but does depend on the network topology and the number of media stream components used for the call (for example, some calls may use Duo Video, or other calls might be audio only).
- Clustered Cisco 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 Cisco VCS's TURN services are supported over single and dual network interfaces. For dual network interfaces, relays are allocated on the Cisco VCS's externally facing LAN interface.
- ICE (Interactive Connectivity Establishment - a mechanism for SIP client NAT traversal) calls can only be made between devices registered to the Cisco VCS's Local Zone.
- Microsoft ICE (which is not standards-based) is not supported.
- The TURN server does not support bandwidth requests. (Note that traversal zone bandwidth limits do not apply.)

Configuring TURN services

TURN relay services are only available on a Cisco VCS Expressway. To use TURN services you also need the TURN Relay option key (this controls the number of TURN relays that can be simultaneously allocated by the Cisco VCS).

The **TURN** page (**VCS configuration > Expressway > TURN**) is used to configure the Cisco VCS Expressway's TURN settings.

The configurable options are:

Field	Description	Usage tips
TURN services	Determines whether the Cisco VCS offers TURN services to traversal clients.	
Port	The listening port for TURN requests. The default is 3478.	If **TURN services** are already enabled, any change to the port number will not come into effect until the **TURN services** are stopped and restarted again.
Authentication realm	The realm sent by the server in its authentication challenges.	Ensure the client's credentials are stored in the device authentication database.
Media port range start / end	The lower and upper port in the range used for the allocation of TURN relays.	

TURN relay status information

The TURN relays page lists all the currently active TURN relays on the Cisco VCS. You can also review further details of each TURN relay including permissions, channel bindings and counters.

Applications

This section provides information about each of the additional services that are available under the **Applications** menu of the Cisco VCS.

You may need to purchase the appropriate option key in order to use each of these applications. They are:

- Conference Factory
- Presence services
- OCS Relay
- FindMe
- Provisioning (Starter Pack)

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 Cisco VCS to support the Multiway feature. Multiway enables endpoint users to create a conference while in a call even if their endpoint does not have this functionality built in.

- Multiway is supported in Cisco TelePresence endpoints including the E20 (software version TE1.0 or later) and MXP range (software version F8.0 or later). 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 the Multiway feature is activated from the endpoint:

1. The endpoint calls a pre-configured alias which routes to the Conference Factory on the Cisco VCS.
2. The Cisco 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**.	

Field	Description	Usage tips
Template	The alias that the Cisco 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 Cisco 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 based upon the upper range limit.)

Note that:

- You must use a different **Template** on each Cisco VCS in your network that has the Conference Factory application enabled. If your Cisco VCS is part of a cluster, the **Template** must be different for each peer in the cluster.
- 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.
- **SIP mode** must be set to *On* (**VCS configuration > Protocols > SIP > Configuration**) 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* (**VCS configuration > Protocols > H.323**), and ensure that **H.323 <-> SIP interworking mode** is set to *Registered only* or *On* (**VCS configuration > Protocols > Interworking**).

Refer to the *Multiway* deployment guide [25] for full details on how to configure individual components of your network (endpoints, MCUs and Cisco VCSs) in order to use Multiway in your deployment.

About Presence

Presence is the ability of endpoints to provide information to other users about their current status - such as whether they are offline, online, or in a call. Any entity which provides presence information, or about whom presence information can be requested, is known as a presentity. Presentities publish information about their own presence status, and also subscribe to the information being published by other presentities and FindMe users.

Endpoints that support presence, such as Movi™ v2.0 (or later) clients, can publish their own status information. The Cisco 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 Cisco 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 Cisco 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

Presence is supported by clustering. For specific information about how Presence information is managed across peers in a cluster, see Clustering and Presence.

Presence Server

The Presence Server application on the Cisco VCS is responsible for managing the presence information for all presentities in the SIP domains for which the Cisco 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 (e.g. another Cisco VCS Control or Expressway).

The Presence Server is made up of the following services, all of which are enabled (or disabled) simultaneously when the Presence Server is enabled (or disabled):

- **Publication Manager**: receives PUBLISH messages, which contain the status information about a presentity, and writes this information to the Presence Database. PUBLISH messages are generated by presence-enabled endpoints and by the Presence User Agent (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 send this information to all subscribers.
- **Presentity Manager**: an interface to the Presence Database. It is used to support Cisco 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 User Agent (PUA)

Endpoints that do not support presence can have status published on their behalf by the Cisco 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 Cisco 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 Cisco 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 Cisco 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 **VCS 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 Cisco 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.

Field	Description
SIP SIMPLE Presence User Agent	*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.

Presence Server

The Presence Server manages the presence information for all presentities in the SIP domains for which the Cisco VCS is authoritative.

Field	Description	Usage tips
SIP SIMPLE Presence Server	*Enabled*: if the local Presence Server is enabled, it will process any PUBLISH messages intended for the SIP domains for which the local Cisco VCS is authoritative. All other PUBLISH messages will be proxied on in accordance with the Cisco VCS's SIP routing rules. Note that SIP routes are configured using the CLI only. *Disabled*: if the local Presence Server is disabled, the Cisco 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 Cisco 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.	

Field	Description	Usage tips
Subscription expiration time	The maximum time (in seconds) within which a subscriber must refresh its subscription. If the subscriber does not send a refresh within this period, the Presence Server will stop sending NOTIFY messages to it. The default is 3600 seconds.	You may want to increase this value in deployments with large numbers of endpoints, to prevent too many messages being sent over your network.
Publication expiration time	The maximum time (in seconds) within which a publisher must refresh its publication. If the publisher does not send a refresh within this period, the Presence Server will show its presence as *Offline*. The default is 1800 seconds.	You may want to increase this value in deployments with large numbers of endpoints, to prevent too many messages being sent over your network.

Regardless of whether or not the Presence Server is enabled, the Cisco 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

Recommendations

- **Cisco VCS Expressway and Cisco VCS Control**: the recommended configuration for a Cisco VCS Expressway when acting as a traversal server for a Cisco VCS Control is to enable the PUA and disable the Presence Server on the Cisco VCS Expressway, and enable the Presence Server on the Cisco VCS Control. This will ensure that all PUBLISH messages generated by the PUA are routed to the Cisco VCS Control.
- **Cisco VCS neighbors**: if you have a deployment with two or more Cisco VCSs neighbored together, you are recommended to enable the presence server on just one Cisco VCS. This will ensure a central source of information for all presentities in your network.
- **Cisco VCS clusters**: for information about how Presence works within a Cisco VCS cluster, see Clustering and Presence.

Note: any defined transforms also apply to any Publication, Subscription or Notify URIs handled by the Presence Services.

OCS Relay

The **OCS Relay** page (**Applications > OCS Relay**) allows you to enable and disable the OCS Relay application on the Cisco VCS, and configure the settings it uses.

The OCS Relay application is required in deployments that use both MOC clients and FindMe, where they both use the same SIP domain. It enables the Cisco VCS to:

- share FindMe presence information with MOC clients
- register FindMe users to a Microsoft Office Communications Server (OCS) so that the OCS can forward calls to FindMe aliases

Note that deployments where the MOC clients and FindMe do not use the same domain do not require use of the OCS Relay application.

Field	Description
OCS Relay mode	Enables and disables the OCS Relay application on the Cisco VCS.
OCS Relay domain	The OCS Relay is used in deployments where MOC clients and FindMe aliases use the same domain. The domain to be used must already be configured on the Cisco VCS (**VCS configuration > Protocols > SIP > Domains**). You can then select the domain from the drop-down menu.
OCS Relay routing prefix	Prefix applied to the SIP domain of requests destined for OCS. This prefix is used by the Cisco VCS search rules to route the requests via the appropriate neighbor zone to the Microsoft Office Communications Server. The default is *ocs*.

The OCS Relay status page (**Status > OCS Relay**) lists all the FindMe aliases being handled by the OCS Relay application, and shows the current status of each.

Configuring a connection between the Cisco VCS and the OCS

To create a connection between the Cisco VCS and the OCS, you must have already configured a neighbor zone on the Cisco VCS with details of the OCS. For the OCS Relay application to be able to route requests to this OCS, you must then:

1. Configure the Cisco VCS with an **OCS Relay routing prefix**.
2. Configure a search rule for the OCS neighbor zone that has a pattern match for that **OCS Relay routing prefix**.
   This ensures that all requests with the specified prefix are routed directly to the OCS.

There are a number of other steps required in order to successfully set up a connection between the Cisco VCS and OCS. These include:

- configuring Call Policy
- configuring Presence

As this is a complex procedure beyond the scope of this guide, you are recommended to refer to the *Microsoft OCS 2007 (R1 and R2) and Cisco VCS Control* deployment guide [24] which describes in detail all the steps required.

About FindMe™

FindMe is a form of User Policy, which is the set of rules that determines what happens to a call for a particular user or group when it is received by the Cisco VCS.

The FindMe feature lets you assign a single FindMe ID to individuals or teams in your enterprise. By logging into their user 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 Cisco VCS's own FindMe manager. However, you can use an off-box FindMe manager; this feature is intended for future third-party integration.

How are devices specified?

When configuring their user 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, it is recommended 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 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; they can only change the **Device name** and **Picture**. This is to stop users from unintentionally changing their basic FindMe configuration.

Principal devices are also used by the Cisco 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 users themselves) can configure which of a user's devices are their principal devices. See Configuring user accounts for more information.

FindMe process overview

When the Cisco 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 Cisco VCS continues to search for the alias in the usual manner.

Note that User Policy is invoked after any Call Policy configured on the Cisco VCS has been applied. See Call routing process for more information.

Who must do what before FindMe can be used?

The following steps are required for the use of FindMe after the feature has been installed:

1. The Cisco VCS administrator:
   a. Enables and configures FindMe.
   b. Must define a cluster name (even if the Cisco VCS is not part of a cluster).
   c. Decides whether to use a local or a remote login account authentication service.
   If remote authentication is being used, the Cisco VCS administrator must also set up User groups.
   d. Creates a user account for each user or team of people who require a FindMe ID.
2. The owner of the FindMe ID configures their account settings.

See the *FindMe* deployment guide [29] for more details on setting up FindMe accounts.

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.

Note: FindMe is supported by clustering. For information about how FindMe information is managed across peers in a cluster, refer to Clustering and FindMe .

Configuring FindMe

The **FindMe configuration** page (**Applications > FindMe > Configuration**) is used to enable and configure FindMe User Policy.

Users configure their FindMe settings by logging into their user account. To configure how user accounts are authenticated, go to the Login account authentication configuration page.

Note that the **FindMe configuration** page can only be accessed if the **FindMe** option key is installed.

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 Cisco VCS's local FindMe manager. *Remote service*: enables FindMe and uses a FindMe manager located on an off-box system. This feature is intended for advanced deployments with third-party integrators.	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	Only applies when **FindMe mode** is *On*. 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 Cisco 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 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.
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>**

The following options apply when **FindMe mode** is *Remote service*:

Field	Description
Protocol	The protocol used to connect to the remote service.
Address	The IP address or domain name of the remote service.
Path	The URL of the remote service.
Username	The username used by the Cisco VCS to log in and query the remote service.
Password	The password used by the Cisco VCS to log in and query the remote service.

Searching for FindMe users

The **User search** page (**Applications > FindMe > Search**) lets you search for user accounts by their related FindMe details such as a FindMe ID or device alias.

This search feature is useful if, for example, you have a device alias but do not know to whom it belongs, or you have a URI and are not sure if it is a FindMe ID or a device alias.

Enter the FindMe ID, username, device address or number you want to search for and click **Search**. Note that the search process performs an exact match against the value entered here — "contains" and wildcard searches are not supported.

All matching user accounts are listed. You can review an account's details by clicking **View/Edit**.

Note that if you are part of a large enterprise with, for example, Cisco TMS managing several Cisco VCS clusters, the search may find users and devices in other Cisco VCS clusters. You can only view (and not edit) the details of accounts that are not managed in your cluster. See Clustering and FindMe for more information.

About provisioning (Starter Pack)

The Cisco VCS's provisioning server provides basic device provisioning for a range of endpoint device types, including Movi users, 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 through the TMS Agent and TMS Provisioning Directory. 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 Cisco VCS functionality and includes the following features:

- Expressway
- FindMe

The following license restrictions apply by default:

- 50 registrations
- 5 calls (any combination of traversal and non-traversal calls); extra call license option keys can be added if required
- 900 TURN relays

When the **Starter Pack** option key is installed the Presence Server and FindMe are enabled by default.

Device authentication

The provisioning server supports device authentication. Provisioned devices' credentials can be authenticated against the Cisco VCS's local authentication database (or the LDAP directory if remote authentication is selected) when they attempt a provisioning request and when they register with the Cisco VCS.

Phone book support

Provisioned devices are served a phone book directory of user accounts.

Configuring provisioning

The **Provisioning** page (**Applications > Provisioning**) is used to configure the Cisco VCS's provisioning server.

The server is automatically enabled when the **Starter Pack** option key is installed.

You can monitor the provisioning server on the Provisioning status page.

Bandwidth limits

The **Provisioning** page 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.

Provisioning users

To provision individual users, you must set up user accounts.

When you configure a user account, you can choose the devices to provision for that user. User accounts are also used to configure a user's FindMe settings.

See the *Cisco VCS Starter Pack Express* deployment guide [34] for full details on setting up Starter Pack provisioning.

Maintenance

This section describes the pages that appear under the **VCS configuration > Maintenance** menu of the Cisco VCS web interface.

These pages allow you to perform the following tasks:

- upgrade to a new release of software
- install and delete option keys
- manage security certificates
- enable advanced account security
- install and select a language pack
- manage administrator and user accounts and passwords
- create and restore backups
- create a system snapshot
- view and configure incident reports
- use built-in tools to check patterns and locate aliases
- view a list of all ports used by the Cisco VCS
- restart, reboot or shut down the Cisco VCS

About upgrading software components

You can install new releases of the Cisco 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 **VCS platform** component using Cisco TMS (see the Cisco TMS documentation for more information).

- To avoid any performance degradation you are recommended to upgrade Cisco VCS components while the system is inactive.
- For specific information about upgrading peers in a cluster, refer to the *Cluster creation and maintenance* deployment guide [27].

Cisco 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 **VCS 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.

Prerequisites

The upgrade requires you to have:

- a valid **Release key**, if you are upgrading to the next major release of the **VCS platform**, for example from X4.1 to X5.0; it is not required for dot releases, for example X5.0 to X5.1
- 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
- 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.

Note: if you later need to downgrade to an X4 (or earlier) release you will have to restore a backup made against that previous release.

Upgrading and option keys

All existing option keys are retained through the upgrade from one version of the **VCS 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 **VCS 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 Cisco VCS software.

Installing and rebooting

Upgrading the **VCS platform** component is a two-stage process. First, the new software image is uploaded onto the Cisco VCS. At the same time, the current configuration of the system is recorded, so that this can be restored after the upgrade. During this initial stage the system will continue running on its existing software version, and all normal system processes will continue.

The second part of the upgrade involves rebooting the system. It is only during the reboot that the Cisco VCS installs the new software version and restores the previous configuration. Rebooting causes all current calls to terminate, and all current registrations to be ended.

This means that you can upload the new software to your system at any time, and then wait until a convenient moment (for example, when no calls are taking place) to install the new version by rebooting the system.

Note: any configuration changes made between the software upload and the reboot will be lost when the system restarts using the new software version.

The upgrade of components other than the **VCS platform** does not involve a system reboot, however the services provided by that component will be temporarily stopped while the upgrade process completes.

Upgrade procedure

The **Upgrade** page (**Maintenance > Upgrade**) is used to install newer (or older) versions of Cisco VCS software components.

To upgrade a component using the web interface:

1. Review the relevant release notes to see if any special steps are required either before or after installing the software image file.
2. Go to the **Upgrade** page (**Maintenance > Upgrade**).
3. Click **Browse** and select the software image file for the component you want to upgrade.
4. Enter the **Release key** if required.
5. Click **Upgrade**.
   The Cisco VCS automatically detects which component you are upgrading based upon the selected software image file.

6. For upgrades to the **VCS platform** component, the **Upgrade confirmation** page is displayed:
   a. Check that the expected **New software version** number is displayed and 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.
   b. Click **Reboot system**. After the reboot is complete you are taken to the **Login** page. Note that if you make any further configuration changes before rebooting, those changes will be lost when the system restarts.
7. For upgrades to other components, the software is automatically installed. No reboot is required.

The upgrade is now complete. The **Overview** and **Upgrade** pages now show the upgraded software component version numbers.

Note that some components may require option keys to enable them; this is done through the Option keys page (**Maintenance > Option keys**).

Downgrading

If you need to downgrade to an X4 (or earlier) release of the **VCS platform**, configuration changes, including changes made to FindMe or Provisioning, will be lost. When the downgrade has completed you will have to restore a backup of the system configuration that was made against the release you have just reinstalled. Other manual steps may be required — you must review the release notes for the version you are downgrading from.

- To downgrade a component to an older release you should follow the same instructions as above for upgrading, but select the appropriate software image file for the software version you want to downgrade to.
- As with upgrading, you are recommended to backup your system configuration before downgrading.

Upgrading using secure copy (SCP/PSCP)

To upgrade using a secure copy program such as SCP or PSCP (part of the PuTTY free Telnet/SSH package) you need to transfer two files to the Cisco VCS:

- A text file containing just the 16-character Release Key (required for the **VCS 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 **VCS 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 **VCS platform** component:
     - Upload to the **/tmp** folder on the system. The target name must be **/tmp/tandberg-image.tar.gz**, for example: **scp s42700x5.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/ocs-relay.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 **VCS platform** component, log in to the Cisco VCS, either using the web interface or CLI, and reboot the Cisco 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.

Option keys

The **Option keys** page (**Maintenance > Option keys**) lists all the existing options currently installed on the Cisco VCS, and allows you to add new options.

Options are used to add additional features to the Cisco VCS. Your Cisco VCS may have been shipped with one or more optional features pre-installed. To purchase further options, contact your Cisco representative.

The **System information** section summarizes the existing features installed on the Cisco VCS. The options that you may see here include:

- *Expressway*: enables the Cisco VCS to work as an Expressway™ firewall traversal server.
- *H.323 to SIP Interworking gateway*: enables H.323 calls to be translated to SIP and vice versa.
- *FindMe*™: enables FindMe functionality.
- *Dual Network Interfaces*: enables the LAN 2 port on your Cisco VCS Expressway.
- *Device Provisioning*: allows Cisco VCS to provision endpoints with configuration information on request and to supply endpoints with phone book information. (Endpoints including Movi v2.0 or later, and E20 v2.1 or later can request to be provisioned.) Note that the Cisco VCS must use Cisco TMS as its external manager to obtain configuration and phone book information for distribution.
- *Starter Pack*: allows the Cisco VCS to offer basic device provisioning for a range of endpoint device types, including Movi users, without the need for Cisco TMS (see Provisioning (Starter Pack)).
- *Traversal calls*: determines the number of traversal calls allowed on the Cisco VCS at any one time. Note that traversal calls that are passing through the Cisco 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 What are traversal calls? section for more information.
- *Non-traversal calls*: determines the number of non-traversal calls allowed on the Cisco VCS at any one time. Note that non-traversal calls that are passing through the Cisco 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 routed mode setting. Note that a non-traversal call on a Cisco 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 Cisco 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 a Cisco VCS, and these will each count as one registration.
- *TURN Relays*: the number of concurrent TURN relays that can be allocated by this Cisco VCS. See About ICE and TURN services for more information.
- *Encryption*: indicates that AES encryption is supported by this software build.
- *Advanced account security*: enables advanced security features and restrictions for high-security installations.
- *Enhanced OCS Collaboration*: enables encrypted calls to and from Microsoft OCS Server 2007 (for both native SIP calls and calls interworked from H323). Note that as the Cisco VCS must process the media in both scenarios, a traversal call license will be used.

Adding option keys using the web interface

To add an option key:

1. In the **Add option key** field, enter the 20-character key that has been provided to you for the option you want to add.
2. Click **Add option**.

Some option keys require that the Cisco VCS is restarted before the option key will take effect. In such cases you will receive a warning on the web interface, which will remain in place as a reminder until the system has been restarted. However, you can continue to use and configure the Cisco 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 certificates

For extra security, you may want to have the Cisco VCS communicate with other systems (such as LDAP servers, neighbor Cisco 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. This certificate must be signed by a Certificate Authority (CA).
- The client must trust the CA that signed the certificate used by the server.

The Cisco VCS allows you to install appropriate files so that it can act as either a client or a server in connections using TLS. The Cisco 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.

- For an endpoint to Cisco VCS connection, the Cisco VCS acts as the TLS server.
- For a Cisco VCS to LDAP server connection, the Cisco VCS is a client.
- For a Cisco VCS to Cisco VCS connection either Cisco VCS may be the client with the other Cisco VCS being the TLS server.
- For HTTPS connections the web browser is the client and the Cisco VCS is the server.

TLS can be difficult to configure. For example, when using it with an LDAP server it is recommended that you confirm that your system is working correctly before you attempt to secure the connection with TLS. You are also recommended to use a third party LDAP browser to verify that your LDAP server is correctly configured to use TLS.

Note: be careful not to allow your CA certificates or CRLs to expire as this may cause certificates signed by those CAs to be rejected.

See Managing security certificates for instructions about how to install certificates. Further information is also available in the *Certificate creation and use with Cisco VCS* deployment guide [32].

Managing security certificates

The **Security certificates** page (**Maintenance > Security certificates**) is used to manage the security certificates used by the Cisco VCS when acting as either a client or a server in connections using TLS, and when authenticating client connections over HTTPS.

Note: certificate and certificate revocation list (CRL) files can only be loaded via the web interface. They cannot be installed using the CLI.

Trusted CA certificate

The **Trusted CA certificate** section manages the list of certificates for the Certificate Authorities (CAs) trusted by this Cisco VCS. Certificates presented to the Cisco VCS must be signed by a trusted CA on this list and there must be a full chain of trust to the root CA.

To upload a new file of CA certificates, **Browse** to the required PEM file and click **Upload CA certificate**. This will replace any previously uploaded CA certificates.

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.

- Click **Reset to default CA certificate** to replace the currently uploaded file with a default list of trusted CA certificates.
- Click **Show CA certificate** to view the currently uploaded file.

Server certificate data

The **Server certificate data** section is used to upload the Cisco VCS's server certificate. This certificate is used to identify the Cisco VCS when it communicates with client systems using TLS encryption, and with web browsers over HTTPS.

- Use the **Browse** buttons to select the **server certificate** PEM file and the **server private key** PEM file that is used to encrypt it. After selecting both files, click **Upload server certificate data**. Note that the private key must not be password protected.
- Click **Reset to default server certificate** to replace the currently uploaded server certificate with the Cisco VCS's default certificate.
- Click **Show server certificate** to view the currently uploaded server certificate file.

HTTPS certificate revocation list (CRL)

You are recommended to upload CRL data for the CAs that sign HTTPS client and server certificates. This is a PEM file that identifies those certificates that have been revoked and can no longer be used to communicate with the Cisco VCS over HTTPS.

Note that CRL checking is applied for every CA in the chain of trust.

- To upload a PEM encoded CRL file, **Browse** to the required file and click **Upload CRL for client certificates**. This will replace any previously uploaded CRL file.
- Click **Remove revocation list** if you want to remove all HTTPS CRL information from the Cisco VCS.

Note that CRL data uploaded here is not used to validate TLS connections with an LDAP server for remote login account authentication. CRL data for this purpose must be contained within the **Trusted CA certificate** file.

Client certificate test

The **Client certificate test** section allows you to check client certificates before enabling client certificate validation.

- To test a certificate, **Browse** to the required PEM file and click **Test client certificate file**. The selected file will be checked against the Cisco VCS's current trusted CA list and, if loaded, the client certificate revocation list. A success or failure message will be displayed.

Advanced account security

The **Advanced account security** page (**Maintenance > Advanced account security**) is used to configure the Cisco VCS for use in highly secure environments.

This page can only be accessed if the **Advanced Account Security** option key is installed.

Enabling advanced account security limits login access to remotely authenticated users using the web interface only, and also restricts access to some Cisco VCS features. To indicate that the Cisco VCS is in advanced account security mode, any text specified as the **Classification banner** message is displayed on every web page.

Note that a system reboot is required for changes to the advanced account security mode to take effect.

Prerequisites

Before advanced account security mode can be enabled, the Cisco VCS must be configured to use remote account authentication for administrator accounts.

Note: ensure that the remote directory service is working properly, as after advanced account security is enabled you will not be able to log in to the Cisco VCS via the local **admin** account or as **root**.

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
- login 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

Warnings are raised for any non-recommended configuration settings.

Cisco VCS functionality: changes and limitations

When in secure mode, the following changes and limitations to standard Cisco VCS functionality apply:

- access over SSH, Telnet, and through the serial port is disabled and cannot be turned on
- access over HTTPS is enabled and cannot be turned off
- the command line interface (CLI) is unavailable
- the root account, the admin account and any other local administrator accounts are disabled
- if there are three consecutive failed attempts to log in (by the same or different users), login access to the Cisco 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 and Configuration Log pages (these pages can only be viewed by accounts with *Auditor* access level)
- the **Upgrade** page only displays the **VCS platform** component
- downgrades to version X5.0 or below are not allowed
- the classification banner is displayed on every web page

Note: the Event Log, Configuration Log, call history, search history and registration history are cleared whenever the Cisco VCS is taken out of advanced account security mode.

Configuring language settings

The **Language** page (**Maintenance > Language**) controls which language is used for text displayed in the web user interface.

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.	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 Cisco VCS user interface using a different browser or a different computer, a different language setting may be in place.

Note:

- You can also get to the **Language** page by clicking on the **Language** link at the bottom of every page.

Language: en_US

- If you upgrade to a later version of Cisco VCS software you may need to install a later version of the associated language pack to ensure that all text is available in the chosen language.

Installing language packs

You can install new language packs or install an updated version of an existing language pack.

To install a language pack:

1. Click **Browse** and select the **.tlp** language pack file you want to upload.
2. Click **Install language pack**.

The selected language pack is then verified and uploaded, and then made available for selection in the **Language** drop-down.

Note that you cannot create your own language packs. Language packs can only be obtained from Cisco. Refer to your Cisco support representative for information on currently available language packs.

About login accounts

The Cisco VCS has two types of login account for normal operation:

- **Administrator accounts**: used to configure the Cisco VCS.

- **User accounts**: used by individuals in an enterprise to configure their FindMe profile. They can also be used to enable basic device provisioning for a range of device types, including Movi users, when the **Starter Pack** option key is installed.

Account authentication

Administrator and user accounts must be authenticated before access is allowed to the Cisco VCS.

The Cisco VCS can authenticate accounts either locally or against a remote directory service, such as Windows Active Directory, using LDAP. The remote option allows administration groups to be set up in the directory service for all Cisco VCSs in an enterprise, removing the need to have separate accounts on each Cisco VCS.

If a remote source is used for either administrator or user account authentication you also need to configure the Cisco VCS with:

- appropriate LDAP server connection settings (see Account authentication using LDAP)
- administrator groups and/or user groups that match the corresponding group names already set up in the remote directory service to manage administrator and user access to this Cisco VCS (see Configuring administrator groups and Configuring user groups)

Administrator accounts

Administrator accounts are used to configure the Cisco VCS. The Cisco VCS has a default **admin** administrator account with full read-write access and can be used to log in to the Cisco VCS using the web interface or the CLI.

You can add additional administrator accounts which can only be used to log in through the web interface.

The default admin account is managed locally and is always accessible, even if remote administrator account authentication is selected. All passwords and usernames are case sensitive.

See the Configuring administrator accounts section for more information.

User accounts

User 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 user account is accessed using a username and password.

- If local user account authentication is selected, each user account must be created locally by a Cisco VCS administrator.
- If remote user account authentication is selected, a Cisco VCS administrator must set up user groups to match the corresponding group names in the remote directory service.

Note that if remote user account authentication is selected, only the username and password details are managed remotely. All other properties of the user account, such as the FindMe ID, devices and locations are stored in the local Cisco VCS database.

See the Configuring user accounts section for more information about defining user account details and their associated FindMe devices and locations, and for enabling basic **Starter Pack** provisioning.

Note: use Cisco TMS if you need to provision a large number of user accounts. See the *FindMe* deployment guide [29] for more details on configuring FindMe and user accounts.

Root accounts

The Cisco VCS provides a root account which can be used to log in to the Cisco 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 the **admin** account instead.

See the Root account section for more information.

Note: remember to change the passwords for the **admin** and **root** accounts from their default values.

Configuring login account authentication

The **Login account authentication configuration** page (**Maintenance > Login accounts > Configuration**) is used to configure where administrator and user account credentials are authenticated before access is allowed to the Cisco VCS.

The **Administrator authentication source** and **User authentication source** options are:

- *Remote*: credentials are verified against an external credentials directory, for example Windows Active Directory. If a *Remote* source is selected you need to configure the appropriate LDAP settings on the Login account LDAP configuration page.
- *Local*: credentials are verified against a local database stored on the Cisco VCS.

After specifying where accounts are authenticated you must set up the appropriate account details or directory service group details. See the *Authenticating Cisco VCS accounts using LDAP* deployment guide [30] for more details on configuring a remote directory service.

Account authentication using LDAP

The **Login account LDAP configuration** page (**Maintenance > Login accounts > LDAP configuration**) is used to configure an LDAP connection to a remote directory service for administrator and/or user account authentication.

To use LDAP for account authentication, you must also go to the Login account authentication configuration page and select a *Remote* administrator or user authentication source.

The configurable options are:

Field	Description	Usage tips
LDAP server configuration: this section specifies the connection details to the LDAP server.		
Server address	The IP address or Fully Qualified Domain Name (or server address, if a DNS Domain Name has also been configured) of the LDAP server to use when making LDAP queries.	
FQDN address resolution	Sets 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*.	

Field	Description	Usage tips
Port	The IP port to use on the LDAP server.	Typically this is 389 for non-TLS, and 636 if TLS encryption is enabled.
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 *Off*.	If you use TLS encryption, you need to upload a suitable CA certificate file. Click **Upload a CA certificate file for TLS** to go to the Security certificates 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 Cisco VCS's authentication credentials to use when binding to the LDAP server.		
Cisco VCS bind DN	The distinguished name used by the Cisco VCS when binding to the LDAP server.	
Cisco VCS bind password	The password used by the Cisco VCS when binding to the LDAP server.	The maximum plaintext length is 60 characters, which is then encrypted.
SASL	The SASL (Simple Authentication and Security Layer) mechanism to use when binding to the LDAP server. *None*: no mechanism is used. *DIGEST-MD5*: the DIGEST-MD5 mechanism is used. The default is *DIGEST-MD5*.	
Cisco VCS bind username	The username used by the Cisco VCS when binding to the LDAP server with SASL.	
Directory configuration: this section specifies the base distinguished names to use when searching for account and group names.		

Field	Description	Usage tips
Base DN for accounts	The distinguished name to use as the base when searching for administrator and user accounts.	
Base DN for groups	The distinguished name to use as the base when searching for administrator and user groups.	

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

See the *Authenticating Cisco VCS accounts using LDAP* deployment guide [30] for more details on configuring an LDAP server, including help on specifying distinguished names for searching the database.

Login history

The **Login history** page is displayed immediately after logging in. It shows the recent activity of the currently logged in account.

Note that this page is only displayed if the account is in advanced account security mode.

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.

Root account

The Cisco VCS provides a root account which can be used to log in to the Cisco 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. A warning is displayed on the web interface and the CLI if the **root** account has the default password set.

Note: the **root** account should not be used in normal operation, and in particular system configuration should not be conducted using this account. Use the **admin** account instead.

Changing the root account password

To change the password for the **root** account:

1. Log in to the Cisco VCS as **root**. By default you can only do this using a serial connection or SSH.
2. Type **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 and Telnet

By default, the root account can be accessed over a serial connection or SSH only - access over Telnet is disabled by default. You may want to enable access over Telnet, but for security reasons this is not recommended.

To enable and disable access to the root account using SSH and Telnet:

1. Log in to the Cisco VCS as **root**.
2. Type one of the following commands:
   - **rootaccess -t on** to enable access using Telnet
   - **rootaccess -t off** to disable access using Telnet
   - **rootaccess -s on** to enable access using SSH
   - **rootaccess -s 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.

Note: if your Cisco VCS is part of a cluster, do not disable root access using SSH. The clustering feature depends on SSH access.

Resetting an administrator or root password

If you forget the password for the default *admin* account or any other administrator account, log in to the Cisco VCS using the account of another administrator with read-write access and change the password.

However, if you do not have any other administrator accounts with read-write access, or have forgotten the passwords for them all, you can set a new password for the *admin* account using the following procedure. This can also be used if you have forgotten the password for the *root* account:

1. Connect a PC to the Cisco VCS using the serial cable as per the instructions in the Cisco VCS Getting Started Guide [28].
2. Restart the Cisco VCS.
3. Log in from the PC with the username **pwrec**. No password is required.
4. Select the account (*root* or *admin*) whose password you want to change.
5. You will be prompted for a new password.

The **pwrec** account is only active for one minute following a restart. After that time you will have to restart the system again to change the password.

Resetting user account passwords

To change a password on behalf of a user without knowing their existing password (for example, when a user forgets their password):

1. Go to the **Edit user account** page (**Maintenance > Login accounts > User 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 user account authentication is enabled. If remote authentication is enabled, passwords are managed through your remote directory server instead.

Configuring administrator accounts

The **Administrator accounts** page (**Maintenance > Login accounts > Administrator accounts**) lists all the administrator accounts that have been configured on the Cisco VCS, and lets you add, edit and delete accounts.

The configurable options are:

Field	Description	Usage tips
Name	The username for the administrator account.	Some names such as "root" are reserved.
Password	The password that this administrator will use to log in to the Cisco VCS. The password can be up to 16 characters.	All passwords on the Cisco VCS are encrypted, so you only see placeholder characters here.
Account access	Administrator accounts can be assigned the following access permissions: *Read-write*: allows all configuration 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** and the **Overview** page only. *Account disabled*: web login access to the Cisco VCS is not allowed.	The access permissions of the currently logged in user are shown in the system information bar at the bottom of each web page.

To create a new administrator account, click **New**.

To edit an existing administrator account, click **View/Edit**.

Password strength

When entering passwords, the bar under the **Password** field changes color to indicate the complexity of the password. If the Cisco VCS is operating in **Enforce strict passwords** mode (set on the Password security page, **Maintenance > Login accounts > Password security**) the password must be *Strong* before it will be accepted.

Note: you cannot set blank passwords for any administrator account.

Default administrator account

The Cisco VCS has a default local administrator account with full *Read-write* access. This account is used to log into the Cisco VCS using the web UI or the CLI.

The username for this account is *admin* (all lower case) and the default password is TANDBERG (all upper case). You cannot delete the default administrator account or change its *admin* username, but you should change the password as soon as possible. Choose a strong password, particularly if administration over IP is enabled.

Administrators can always log in using the local *admin* account even if remote administrator authentication is enabled. If you forget the password for the *admin* account, you can still log in as another administrator user with read-write access and change the password for the *admin* account.

If you do not have any other such administrator users set up, or you have forgotten those passwords as well, it is possible to reset the password for the admin account as long as you have physical access to the Cisco VCS. See the Resetting an administrator or root password section for details.

Additional administrator accounts

You can add up to 15 additional administrator accounts, which can be used to log in to the web user interface but not the CLI. If remote administrator authentication is enabled, only the local *admin* account is displayed.

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.

Password security

The **Password security** page (**Maintenance > Login accounts > Password security**) controls whether or not administrator passwords must meet a minimum level of complexity before they are accepted.

If **Enforce strict passwords** is set to *On*, all subsequently configured administrator passwords must contain at least 15 ASCII characters made up of at least:

- 2 lowercase letters ['a'..'z']
- 2 uppercase letters ['A'..'Z']
- 2 numeric values ['0'..'9']
- 2 special characters [such as '@' or '$']

If **Enforce strict passwords** is set to *Off*, no checks are made on administrator passwords.

Note that:

- Regardless of this setting, it is not possible to set a blank password for any administrator account.
- This setting affects administrator passwords only. It does not affect any other passwords used on the Cisco VCS such as in the local authentication database, LDAP server, external registration credentials or user account passwords.
- All passwords and usernames are case sensitive.

Configuring administrator groups

The **Administrator groups** page (**Maintenance > Login accounts > Administrator groups**) lists all the administrator groups that have been configured on the Cisco VCS, and lets you add, edit and delete groups.

Note: administrator groups are only active when remote administrator authentication is enabled.

Administrator groups determine which access rights members of the group have after they have been successfully authenticated to use the Cisco VCS.

When an administrator logs in to the Cisco VCS web interface, their credentials are authenticated against the remote directory service and they are assigned the access rights associated with the group to which the administrator belongs. 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 Cisco VCS must match the group names that have been set up in the remote directory service to manage administrator access to this Cisco VCS.
Access	The access level for members of the specified administrator group: *Read-write*: allows all configuration 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** and the **Overview** page only. *None*: web login access to the Cisco VCS is not allowed.	

To create a new administrator group, click **New**.

To edit an existing administrator group, click **View/Edit**.

Configuring user accounts

The **User accounts** page (**Maintenance > Login accounts > User accounts**) lists all the user accounts that have been configured on the Cisco VCS, and lets you add, edit and delete accounts.

User 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 user account is accessed using a username and password.

- If local user account authentication is selected, each user account must be created locally by a Cisco VCS administrator.
- If remote user account authentication is selected, the Cisco VCS administrator must set up user groups to match the corresponding group names in the remote directory service.

The configurable options for a user 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 Cisco 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 Cisco VCS must match the username set up in the remote directory service.

Field	Description	Usage tips
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 the *FindMe* deployment guide [29] 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 it is recommended 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 users themselves) can add more endpoint addresses after an account has been created.	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.
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.

Principal devices (Starter Pack only)

The **Principal devices** section is used to specify the principal devices that are associated with the FindMe user 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 user 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 a Movi device would be **alice.smith.movi@example.com**.

- Each selected device is automatically provisioned (with bandwidth limits and phone book information, for example) when that device registers to the Cisco 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 user account** page.
- 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 to able to delete that device. To do this, click **Edit principal devices** from the **Edit user account** page. You can then configure which of the user's devices are principal devices.

Note that the Cisco VCS only sends provisioning information to the pre-configured device types (Movi, 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 Cisco VCS.

If device authentication using a local database is enabled, authentication credentials for the provisioned devices must also be set up in the local authentication 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.

Note: all device address URIs are converted to lower case.

Multiple Cisco VCS clusters

If you are part of a large enterprise with, for example, Cisco TMS managing several Cisco VCS clusters, the database may contain details of users and devices in other Cisco VCS clusters. Different clusters are distinguished by their **Cluster name**. You cannot modify the details of accounts that are not managed in your cluster.

Configuring a user's principal devices

The **Edit principal devices** page (**Maintenance > Login accounts > User accounts**, click **View/Edit** or the username to open the **Edit user 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.

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 Cisco 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.

Configuring user groups

The **User groups** page (**Maintenance > Login accounts > User groups**) lists all the user groups that have been configured on the Cisco VCS, and lets you add, edit and delete groups.

Note: user groups are only active when remote user authentication is enabled.

User groups determine which access rights members of the group have after they have been successfully authenticated to use the Cisco VCS.

When a user logs in to the Cisco 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 user group. It cannot contain any of the following characters: / \ [ ] : ; | = , + * ? > < @ "	The group names defined in the Cisco VCS must match the group names that have been set up in the remote directory service to manage user accounts.
Access	The access level for members of the specified user group: *Read-write*: users can view and modify their personal FindMe details, devices and locations. *None*: users are not allowed to log in to their account.	

To create a new user group, click **New**.

To edit an existing user group, click **View/Edit**.

Backing up and restoring Cisco VCS data

The **Backup and restore** page (**Maintenance > Backup and restore**) is used to create and restore backup files of your Cisco VCS data.

You are recommended to create a backup in the following situations:

- before performing an upgrade
- before performing a system restore
- in demonstration and test environments if you want to be able to restore the Cisco VCS to a known configuration

You can independently backup and restore two different sets of data:

System data, which includes:

- system configuration settings
- Call Policy
- clustering configuration
- security certificates
- administrator account details
- user accounts and FindMe settings (when the *Starter Pack* option key is installed)

TMS Agent data, which includes:

- user accounts and FindMe settings (when the *Starter Pack* option key is not installed)
- TMS Agent provisioning accounts and settings

Note that event logs are not included in the backup files.

Limitations

- Backups can only be restored to a Cisco VCS running the same version of software from which the backup was made.
- You can create a backup on one Cisco VCS and restore it to a different Cisco VCS, for example if the original system has failed. However, before performing the restore you must install on the new system the same set of option keys that were installed on the old system. If you attempt to restore a backup made on a different Cisco VCS, you will receive a warning message, but you will be allowed to continue.
- Backups should not be used to copy data between Cisco VCSs.

Note: you are recommended to take the Cisco VCS unit out of service before performing a restore.

For extra information about backing up and restoring peers in a cluster, refer to the Cluster backup and restore section.

Creating a backup

System data

To create a backup of the Cisco VCS's **System** data:

1. Go to the **Backup and restore** page (**Maintenance > Backup and restore**).
2. Click **Create system backup file**.
3. After the backup file has been prepared, a pop-up window appears and prompts you to save the file (the exact wording depends on your browser). The default name is in the format: **<hardware serial number>_<date>_<time>_backup.tar.gz**.
4. Save the file to a designated location.

TMS Agent data

To create a backup of the Cisco VCS's **TMS Agent** data:

1. Go to the **Backup and restore** page (**Maintenance > Backup and restore**).
2. Click **Create TMS Agent backup file**.
3. After the backup file has been prepared, a pop-up window appears and prompts you to save the file (the exact wording depends on your browser). The default name is in the format: **<date>_<time>_tms_agent_backup.tar.gz**.
   Note that the preparation of the TMS Agent backup file may take several minutes. Do not navigate away from this page while the file is being prepared.
4. Save the file to a designated location.

The preparation of the TMS Agent backup file may take several minutes. Do not navigate away from this page while the file is being prepared.

Restoring a previous backup

System data

To restore the Cisco VCS to a previous configuration of **System** data:

1. Go to the **Backup and restore** page (**Maintenance > Backup and restore**).
2. In the **Restore** section, **Browse** to the backup file containing the configuration you want to restore.
3. Click **Upload system backup file**.
4. The Cisco VCS checks the file and takes you to the **Restore confirmation** page.
   - If the backup file is not valid, you will receive an error message at the top of the **Backup and restore** page.

   You are shown the current software version and the number of calls and registrations.

5. Read all the warning messages that appear before proceeding with the restore.
6. Click **Continue with system restore** to continue with the restore process. This will restart your system, so ensure that there are no active calls.
   - Click **Abort system restore** if you need to exit the restore process and return to the **Backup and restore** page.

After the system restarts, you are taken to the login page.

TMS Agent data

To restore the Cisco VCS to a previous set of **TMS Agent** data:

1. Go to the **Backup and restore** page (**Maintenance > Backup and restore**).
2. In the **Restore** section, **Browse** to the backup file containing the configuration you want to restore.
3. Click **Upload TMS Agent backup file**.
4. The Cisco VCS checks the file and restores its contents.
   - If the backup file is not valid, you will receive an error message at the top of the **Backup and restore** page.

Creating a system snapshot

The **System snapshot** page (**Maintenance > System snapshot**) allows you to create a file that can be used for diagnostic purposes. The file should be sent to your Cisco support representative at their request to assist them in troubleshooting issues you may be experiencing.

To create a system snapshot file:

1. Click **Create system snapshot** to start the download of the system snapshot file.
   The preparation of the snapshot file may take several minutes to complete.
2. When the file has been created, 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 Cisco support representative.

Incident reporting

The incident reporting feature of the Cisco VCS automatically saves information about critical system issues such as application failures. You can:

- configure the Cisco VCS to send the reports automatically to Cisco
- view the reports from the Cisco 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.

This feature is only intended for use at the request of Cisco customer support in exceptional situations, and is off by default.

Incident reporting warning: 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 CISCO 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.

Sending incident reports automatically

Please read the privacy-protected personal data warning before you decide whether to enable automatic incident reporting.

To configure the Cisco VCS to send incident reports automatically to Cisco customer support:

1. Go to the **Incident reporting configuration** page (**Maintenance > 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.

Note that 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 from the **Incident view** page.

Sending incident reports manually

Please read the privacy-protected personal data warning 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 the **Incident view** page (**Maintenance > 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 > Incident reporting > View**) shows a list of all incident reports that have occurred since the Cisco 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 Cisco VCS software version running when the incident occurred.
Build	The internal build number of the Cisco VCS software version running when the incident occurred.
State	The current state of the incident: *Pending*: indicates that the incident has been saved locally but not sent. *Sent*: indicates that details of the incident have been sent to the URL specified in the Incident reporting 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 > 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 > 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 Cisco VCS software version running when the incident occurred.
Build	The internal build number of the Cisco VCS software version running when the incident occurred.

Field	Description
Name	The name of the software.
System	The configured system name.
Serial number	The hardware serial number.
Process ID	The process ID the Cisco VCS application had when the incident occurred.
Release	A true/false flag indicating if this is 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.

Warning: 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, please read the warning regarding privacy-protected personal data before you decide whether to enable automatic incident reporting.

Checking the effect of a pattern

The **Check pattern** page (**Maintenance > Tools > Check pattern**) lets you test whether a pattern or transform you intend to configure on the Cisco 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 Cisco VCS
- Cisco AM GW policy rules to determine which calls are routed via the Cisco AM GW

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**.
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 transformed alias if appropriate.

Locating an alias

The **Locate** page (**Maintenance > Tools > Locate**) lets you test whether the Cisco 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 Cisco 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. Enter the **Source 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.
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 or a directory service 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 Cisco VCS received a call request from the selected **Source zone**. For more information, see the Call routing process section.

Port usage

The pages under the **Maintenance > Tools > Port usage** menu show, in table format, all the IP ports that have been configured on the Cisco VCS.

The information shown on these pages is specific to that particular Cisco VCS and varies depending on the Cisco 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 Cisco 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 Cisco VCS configuration.

The port information is split into the following pages:

- Local VCS inbound ports
- Local VCS outbound ports
- Remote listening ports

On a Cisco VCS Expressway you can also configure the specific listening ports used for firewall traversal by going to the Ports page (**VCS configuration > Expressway > Ports**).

Further information about ports can be found in the Port reference section.

Local VCS inbound ports

The **Local VCS inbound ports** page (**Maintenance > Tools > Port usage > Local VCS inbound ports**) shows the listening ports on this Cisco VCS. These are the IP ports on the Cisco VCS used to receive inbound communications from other systems.

For each port listed on this page, if there is a firewall between the Cisco VCS and the source of the inbound communications, your firewall must allow:

- inbound traffic to the IP port on the Cisco VCS from the source of the inbound communications, and
- return traffic from that same Cisco VCS IP port back out to the source of the inbound communication.

Note: this firewall configuration is particularly important if this Cisco VCS is a traversal client or traversal server, in order for Expressway firewall traversal to function correctly.

Local VCS outbound ports

The **Local VCS outbound ports** page (**Maintenance > Tools > Port usage > Local VCS outbound ports**) shows the source IP ports used by this Cisco VCS. These are the IP ports on the Cisco VCS used to send outbound communications to other systems.

For each port listed on this page, if there is a firewall between the Cisco VCS and the destination of the outbound communications, your firewall must allow:

- outbound traffic out from the IP port on the Cisco VCS to the destination of the outbound communications, and
- return traffic from that destination back to the same Cisco VCS IP port.

Note: this firewall configuration is particularly important if this Cisco VCS is a traversal client or traversal server, in order for Expressway firewall traversal to function correctly.

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 Cisco VCS communicates.

Your firewall must be configured to allow traffic originating from the local Cisco 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 Cisco VCS will be sending media and signaling, but the ports on which these devices receive traffic from the Cisco 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 VCS outbound ports page, the Cisco 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.

Restarting

The **Restart** page (**Maintenance > Restart**) allows you to restart the Cisco VCS without having physical access to the hardware.

WARNING: do not restart the Cisco VCS while the red ALM LED on the front of the box is on. This indicates a hardware fault. Contact your Cisco representative.

The restart function shuts down and restarts the Cisco VCS application software, but not the operating system or hardware. Some configuration changes require a restart of the Cisco VCS before they take effect. A **Restart** button is at the bottom of any web page that includes such settings, and clicking it takes you to the **Restart** page. A system warning will remain in place until the system is restarted.

Restarting causes any active calls and registrations to be terminated. For this reason, the **Restart** section displays the number of current calls and registrations, so you can check these before you restart the Cisco VCS. If you do not restart the system immediately, you should refresh this page before restarting to check the current status of calls and registrations.

Restarting using the web interface

To restart the Cisco VCS using the web interface:

1. Go to **Maintenance > Restart**, or from a relevant configuration page, click the **Restart** button. You are taken to the **Restart** page.
2. Check the number of calls and registrations currently in place.
3. Click **Restart system**.
   The **Restarting** page appears, with an orange bar indicating progress.

After the system has successfully restarted, you are automatically taken to the **Login** page.

Note: to shut down and restart the Cisco VCS operating system and hardware in addition to the Cisco VCS application software, choose the Reboot function (**Maintenance > Reboot**). Restarting is quicker than rebooting.

Rebooting

The **Reboot** page (**Maintenance > Reboot**) allows you to reboot the Cisco VCS without having physical access to the hardware.

WARNING: do not reboot the Cisco VCS while the red ALM LED on the front of the box is on. This indicates a hardware fault. Contact your Cisco representative.

The reboot function shuts down and restarts the Cisco VCS application software, operating system and hardware. Reboots are normally only required after software upgrades and are performed as part of the upgrade process.

Rebooting will cause any active calls and registrations to be terminated. For this reason, the **Reboot** section displays the number of current calls and registrations, so you can check these before you reboot. If you do not reboot the system immediately, you should refresh this page before rebooting to check the current status of calls and registrations.

Rebooting using the web interface

To reboot the Cisco VCS using the web interface:

1. Go to **Maintenance > Reboot**. You are taken to the **Reboot** page.
2. Check the number of calls and registrations currently in place.
3. Click **Reboot system**.
   The **Rebooting** page appears, with an orange bar indicating progress.

After the system has successfully rebooted, you are automatically taken to the **Login** page.

Note: to shut down and restart the Cisco VCS application software but not the operating system and hardware, choose the restart function (**Maintenance > Restart**). Restarting is quicker than rebooting, but you may want to perform a reboot if a restart has not had the desired effect.

Shutting down

The **Shutdown** page (**Maintenance > Shutdown**) allows you to turn off the Cisco VCS without having physical access to the hardware.

WARNING: do not shut down the Cisco VCS while the red ALM LED on the front of the box is on. This indicates a hardware fault. Contact your Cisco representative.

The system must be shut down before it is unplugged.

After the system has been shut down, the only way it can be restarted 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.

Shutting down causes any active calls and registrations to be terminated. For this reason, the **Shutdown** section displays the number of current calls and registrations, so you can check these before you shutdown. If you do not shut down the system immediately, you should refresh this page before shutting down to check the current status of calls and registrations.

Shutting down using the web interface

To shut down the Cisco VCS:

1. Go to **Maintenance > Shutdown**. You are taken to the **Shutdown** page.
2. Check the number of calls and registrations currently in place.
3. Click **Shutdown system**.
   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 Cisco VCS will be unsuccessful.

Shutting down using the CLI

The Cisco VCS cannot be shut down using the CLI.

Reference material

This section provides supplementary information about the features and administration of the Cisco VCS, including:

- Event Log levels and messages
- CPL reference and examples
- LDAP configuration for device authentication
- DNS configuration
- password encryption
- pattern matching variables
- port reference
- regular expression reference
- supported characters
- TMS agent and TMS agent passwords
- what constitutes traversal calls
- using the command line interface (CLI)
- restoring the system to its default settings
- warnings
- bibliography
- glossary

Software version history

This section summarizes feature updates that have occurred in earlier software releases.

- X5.2
- X5.1
- X5
- X4

X5.2

Telephone event interworking

The Cisco VCS now supports the interworking of DTMF events between SIP and H.323. This allows SIP devices to dial into PIN protected conferences and to select conferences using the DTMF menu.

There are the following limitations:

- 4 Audio packets are dropped each time DTMF is interworked from H323 to SIP. This means that DTMF will only work if there are audio packets flowing from H323 to SIP.
- The duration of events is not interworked, only fixed constants are supported.

Encrypted calls to Microsoft OCS Server 2007

Encrypted calls to and from Microsoft OCS Server 2007 for both native SIP calls and calls interworked from H323 are now supported. This feature is enabled by the **Enhanced OCS Collaboration** option key. Note that as the Cisco VCS must process the media in both scenarios, a traversal call license is used.

Message waiting indication

The Cisco VCS now supports forwarding of unsolicited NOTIFY messages to registered endpoints. This allows message waiting indication from CUCM to be forwarded to E20s thus allowing the indicator light to flash.

Ports

The Cisco VCS no longer listens on multicast/port 1718 when **H.323 Gatekeeper Auto discover mode** is set to *Off* (this has the effect of disabling IGMP messages).

Call bandwidth

The maximum value for the default call bandwidth on a Cisco VCS has been increased from 2048 kbps to 65535 kbps.

Presence

Default timers for the Presence User Agent retry attempts have been increased to prevent resources being consumed.

- The default **Subscription expiration time** has increased from 300 to 3600 seconds.
- The default **Publication expiration time** has increased from 120 to 1800 seconds.
- The default **PUA resend time** (not configurable through the web interface) has increased from 5 to 1800 seconds.

X5.1

Usability enhancements

- **Description fields for configuration items**: a free-format description can be specified for the following configuration items: transforms, Allow List and Deny List patterns, search rules, subzone membership rules. When viewing the summary list of these items the description is displayed as a mouse-over tooltip.
- **Enable and disable configuration items**: transforms, search rules and subzone membership rules can be individually enabled and disabled. This makes it easier to make or test configuration changes. Previously, configuration items would have to be deleted and re-created as necessary. The enabled or disabled state is clearly shown on the summary list pages.
- **"Add suffix" and "add prefix" transform options**: new presearch transform pattern behavior options let you add a prefix or suffix to the matching alias. Previously, regular expressions would have been required to do this.
- **Consistent create and modify behavior for configuration items**: for configuration where multiple items can be defined (for example, Allow List patterns, search rules and so on) the create and modify behavior has been made consistent so that you are always returned to the summary list page after saving your changes.
  Additionally, new search rules, subzone membership rules, subzones and zones are all created in a single step. Previously you had to specify some of the configuration values when creating the item, and then return to the edit page to specify the remainder of the values.
- **"Please select" in drop-down fields**: when creating configuration items some of the default values presented in drop-down selection fields have been replaced with a "please select" value. This helps prevent potentially undesirable default values being selected by mistake.
- **Improved filtering options for Event Log and Configuration Log**: advanced filtering options let you include or exclude specific words or phrases when filtering the view of the Event Log and the Configuration Log.
- **OCS Relay status**: colored status icons make the difference between the online and offline OCS Relay status more distinct.
- **Configuration warnings**: more warnings are raised for common misconfiguration scenarios, for example if a clustered Cisco VCS has H.323 disabled, or if default links are not present.

FindMe™ / User Policy option key

- The User Policy option key has been renamed as the FindMe™ option key.
- "FindMe accounts" and "FindMe groups" are now referred to as "user accounts" and "user groups" respectively.

Subzone registration policies

- In addition to using Allow Lists and Deny Lists, registrations can be controlled at the subzone level. Each subzone can be configured to allow or deny registrations assigned to it via the subzone membership rules.
- Up to 3000 subzone membership rules (previously 2000) can be configured across all subzones.

Zone configuration

- **TLS authentication**: the Cisco VCS can perform certificate verification of neighbor zones when communicating over TLS. Mutual authentication can be performed with neighbor Cisco VCSs.
- **TLS default transport type**: TLS is the default SIP transport type when setting up new neighbor, traversal client and traversal server zones.
- **SIP authentication trust**: the Cisco VCS can be configured to trust incoming SIP messages from specified neighbor zones, rather than challenge them. This applies even if device authentication is enabled on the Cisco VCS.
- **Accept proxied registrations**: controls whether proxied SIP registrations routed through a neighbor, traversal client or traversal server zone are accepted.

- **Nortel Communication Server 1000 zone profile**: the Cisco VCS can automatically configure the settings required for connections to a Nortel Communication Server 1000.
- **Separate authentication credentials per traversal client zone**: each traversal client zone specifies its own username and password for authentication with the traversal server. This allows a traversal client Cisco VCS to connect to one or more service providers. Note that the existing **Outbound connection credentials** username and password are still used for connections to all other (non traversal server) external systems.

Conference Factory generated alias ranges

- The upper and lower range limits of the numeric portion of the generated alias can be specified.
- The numeric portion of the generated alias will pad with leading zeroes to maintain a constant length, for example a range of 10-999 will generate aliases 010 through 999.

Cisco TelePresence Advanced Media Gateway support

The Cisco TelePresence Advanced Media Gateway (Cisco AM GW) provides support for transcoding between standard codecs (such as H.264) and Microsoft RT Video to allow high definition calls between Microsoft Office Communicator (MOC) clients and Cisco endpoints.

- Advanced Media Gateway zone profile: automatically configures the Cisco VCS with the zone settings required for connection to an Cisco AM GW.
- Policy rules: ability to define policy rules to control whether all or only selected calls to or from MOC clients are diverted through the Cisco AM GW.

Far end camera control interworking

The Cisco VCS supports far end camera control (FECC) when interworking calls between SIP and H.323 endpoints.

G.729 support for interworked calls

The G.729 codec is supported for interworked calls.

Advanced account security

An Advanced account security option key enables advanced security features and restrictions for high-security installations.information about this feature.

CRL checking for TLS connections to LDAP servers

Certificate revocation lists (CRLs) can be uploaded and used to verify certificates presented by an LDAP server to the Cisco VCS when forming a TLS connection.for more information.

HTTPS client certificate validation

- The Cisco VCS web server can be configured to request a valid client certificate before establishing an HTTPS session with a client system (typically a web browser).
- Client certificate revocation lists can be uploaded and used to verify the client certificate.

Clustering

- **Improved resilience**: cluster configuration replication is more resilient to network delay.
- **TURN server**: relay allocation requests are redirected to other cluster peers if the first Cisco VCS's relays are fully allocated.

Hardware failure warnings

Improved hardware failure detection, warnings and status display.

Auditor account access level

An **Auditor** access level can be assigned to administrator accounts and groups. Users with the Auditor privilege can only access the **Overview**, **Event Log** and **Configuration Log** pages.

Remote account authentication over LDAP

The LDAP server address of the remote directory service can be specified as a DNS SRV record, thus allowing multiple (primary and backup) servers to be specified.

Starter Pack

The **Starter Pack** option key is only available as a pre-configured factory setting. It is designed for single box deployments and provides basic device provisioning for registered Movi users, without the need for Cisco TMS. It supports device authentication and supplies phone book information to provisioned devices.

The Starter Pack includes the following features:

- Expressway
- FindMe

It has the following license restrictions:

- 50 registrations
- 5 calls (any combination of traversal and non-traversal calls)

Note that installing additional call license option keys will have no effect while the Starter Pack option key is present.

X5

Enterprise authentication

The Cisco VCS can authenticate administrator and/or FindMe accounts against a remote directory service, such as Windows Active Directory, over LDAP. This allows administration groups to be set up in the directory service for all Cisco VCSs in an enterprise, removing the need to have separate accounts on each Cisco VCS.

FindMe™ enhancements

- FindMe account users can set up a list of locations such as "at home" or "in the office" and associate their personal devices with those locations. Only those devices associated with their currently active location will ring when their FindMe is called.
- You can display the caller's **FindMe ID** as the **Caller ID** associated with the originating endpoint's address. This 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 displayed instead.
- Administrators can specify text to display to all FindMe users when they configure a device on their FindMe account.
- A new **FindMe search** page lets you search for FindMe usernames and aliases.

Include ISDN gateway prefix on caller ID display

On the **H.323** configuration page you can specify whether the **Caller ID** displayed on the destination endpoint includes the prefix of the ISDN gateway when displaying the caller's E.164 number.

Subzone configuration

- Cisco VCS now supports up to 1000 subzones (previously 200).
- You can now configure up to 2000 membership rules across all subzones, replacing the previous method of specifying up to five IP subnets per subzone. Each rule can specify either an IP subnet as before or an alias pattern match.
- Number of pipes increased from 100 to 1000.
- Number of links increased from 600 to 3000.

Zone configuration

- Cisco VCS now supports up to 1000 zones (previously 200).
- New **Cisco Unified Communications Manager** zone profile option configures the settings required for connections to a Cisco UCM.

Zone matches replaced by search rules

Instead of specifying up to 5 matches when configuring a zone, you now set up separate search rules and associate each rule with a target zone to where the query is forwarded.

- You can configure up to 2000 search rules.
- A **Stop searching** option makes the search process more efficient by allowing you to stop searching any further zones when a search rule results in a successful match.
- A **Source** option lets you control whether a search rule is applied depending on the source of the query.
- The **Calls to unknown IP addresses** and **Fallback alias** configuration settings have moved from the **Calls** page to a new **Search rules configuration** page.

Quality of Service

The Cisco VCS supports the DiffServ (Differentiated Services) Quality of Service mechanism for tagging all signaling and media packets flowing through the Cisco VCS over IPv4 and IPv6 protocols.

Expressway call licensing

A non-traversal call on a Cisco VCS Expressway now consumes a traversal license if there are no non-traversal call licenses available.

Microsoft Office Communications Server 2007 integration

- The OCS Relay application is now supported in a Cisco VCS cluster and with an OCS cluster.
- OCS Director is now supported.

TURN server

A Cisco VCS Expressway can act as a standards-based TURN server, allowing ICE-enabled endpoints to traverse NAT firewall devices.

- TURN services do not consume traversal call licenses but instead you need to install the **TURN Relay** option key which controls the number of TURN relays that can be simultaneously allocated by the Cisco VCS.
- This replaces the STUN Relays used in version X4 (which consumed traversal call licenses).

CPL

The **rule** node supports a **message-regex** parameter that allows a regular expression to be matched against an incoming SIP message. Note that this parameter does not apply to H.323 calls.

Cisco VCS warnings display as Cisco TMS trouble tickets

Warnings raised on the Cisco VCS are also raised as Cisco TMS tickets.

Call media statistics

Improved media statistics can be viewed on the **Call media** page:

- counters are now per call rather than per socket
- lost, duplicate and out of order packet counts
- jitter on each RTP channel in a call

Clustering

- A **Cluster name** is used to identify one cluster of Cisco VCSs from another.
  - You must define a Cluster name if you are using FindMe, even if the Cisco VCS is not part of a cluster.
  - If you change the Cluster name after creating your FindMe accounts you will have to reconfigure those FindMe accounts for that new name.
- H.323 endpoints are presented with a randomly ordered list of peers, ensuring endpoints that can only store a single alternate peer will failover evenly across the cluster.

Separate backup files for TMS Agent database

The backup and restore of the TMS Agent database (FindMe and TMS Agent provisioning accounts and settings data) is now separate from the main Cisco VCS system configuration backup files.

Hardware status

A **Hardware** page provides information about the physical status of your Cisco VCS unit.

Restart and reboot

The Cisco VCS now distinguishes between a restart function which is required for some configuration changes to take effect, and a full reboot process which is only required after a software upgrade.

Upgrade of Cisco VCS components

You can now upgrade individual Cisco VCS components separately. The main component is the **VCS platform**, and when upgraded will typically include automatic upgrades of some or all of the other components.

Administrator tools

- The **Locate** test tool lets you specify the zone from which to simulate the origin of the search request.
- The **Port usage** tools let you export port usage details in a CSV format file suitable for reviewing in a spreadsheet application.

System configuration

- An **External LAN interface** field is used to indicate on the **IP** page which LAN port has been connected to your external network. It also determines the port from which TURN server relay allocations are made.
- On the **DNS** page you can now specify the **Local host name**. This is the DNS host name that this Cisco VCS is known by.
- The **NTP server** field on the **Time** page now defaults to one of four NTP servers provided by Cisco, either: 0.ntp.tandberg.com, 1.ntp.tandberg.com, 2.ntp.tandberg.com or 3.ntp.tandberg.com.

SIP configuration

New parameters have been added to the SIP configuration page.

- SIP session expiry timers can be configured through the **Session refresh interval** and **Minimum session refresh interval** settings.

- SIP device interoperability can now be configured through the **Require UDP BFCP mode** and **Require Duo Video mode** settings. Note that the default setting of On for these modes is not supported by some neighbor systems so make sure you select the appropriate Zone profile when configuring zones.

X4

Multiway™

Cisco VCS now supports standards-based Multiway™. This feature allows endpoint users to initiate ad hoc multiparty calls from their endpoint, -even if the endpoint does not have embedded MultiSite™ capabilities. To enable this feature you must enable and configure the Conference Factory application on the Cisco VCS.

TMS Agent

The TMS Agent allows Movi™ v2.0 clients registered to the Cisco VCS to be provisioned with phone book and configuration information by connecting to the Cisco VCS rather than directly to Cisco TMS.

Microsoft OCS 2007 interoperability

- The Cisco VCS now includes an OCS Relay application, which makes FindMe presence information available to Microsoft Office Communicator (MOC) clients, and enables Microsoft Office Communications Server (OCS) 2007 to forward calls to FindMe aliases.
- Neighbor and DNS zones now include a pre-configured zone profile for connections to an OCS.

Static NAT support

A Cisco VCS Expressway with the Dual Network Interfaces option installed can now be deployed in a DMZ with a static private address mapped to a public IP address of the external firewall.

Password security

- You can determine whether or not administrator passwords must meet a minimum level of complexity before they are accepted.
- The **admin** administrator account and the **root** account can now have separate passwords.
- A warning will appear if the password of the default admin administrator account or the root account are still set to the default.

Root account access

Access to the root account using Telnet and SSH can be disabled to increase security on the Cisco VCS (access over Telnet is now disabled by default).

Capacity warnings

The Cisco VCS can now raise a warning when it is approaching its maximum licensed capacity for calls or registrations. This feature is managed using the CLI only using the command:
ResourceUsage Warning Activation Level: <0..100>

Clustering

The replication of configuration information (including FindMe information) no longer requires the use of Cisco TMS. Information is replicated across the peers in a cluster within 60 seconds.

Call processing

- The Cisco VCS has a new **Call routed mode** which will determine whether or not it will attempt to remove itself from the call signaling path.

- The Cisco VCS has a new **Call loop detection mode** which can be configured to detect and stop loops from happening during the search phase for both H.323 and SIP.

Administrator tools

- The **Check pattern** tool allows you to test the outcome of a pattern or transform before configuring it live on the Cisco VCS.
- The **Locate** tool allows you to test whether the Cisco VCS can find an endpoint identified by a given alias, within a specified number of 'hops', without actually placing a call to that endpoint. This tool can be used to diagnose dial plan and network deployment issues.
- The **Port usage** pages provide a convenient way to see a complete list of all inbound, outbound and remote listening ports used by the Cisco VCS. This information can be provided to your Firewall Administrator to ensure the correct ports are opened on the firewall.

Usability enhancements

- In addition to the existing help for every input field, there is now help available for every page on the web interface. This help gives an overview of the purpose of the page, and introduces any concepts configured from the page including when they may be used.
- Registrations can now be viewed either as a list of all devices that have registered regardless of the aliases they have used, or as a list of every alias registered on the Cisco VCS, regardless of whether these belong to the same device.

Login banner

You can upload an image and text that will be displayed when administrators or FindMe users log in the Cisco VCS.

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
Level 1	High-level events such as registration requests and call attempts. Easily human readable. For example: ▪ call attempt/connected/disconnected ▪ registration attempt/accepted/rejected
Level 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
Level 3	All Level 1 and Level 2 Events, plus: ▪ protocol keepalives ▪ call-related SIP signaling messages
Level 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 Cisco 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.
process_name	The name of the program generating the log message. This could include: ▪ **tvcs** for all messages originating from Cisco VCS processes ▪ **findme** for FindMe account data migration events ▪ **web** for all web login and configuration events ▪ **tprovisioning** for all events associated with the TMS Agent but will differ for messages from other applications running on the Cisco 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 Cisco VCS, and the level at which they are logged.
User	The username that was entered when a login attempt was made.
ipaddr	The source IP address of the user who has logged in.
Protocol	Specifies which protocol was used for the communication. Valid values are: ▪ 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.

Name	Description
Response-code	SIP response code or, for H.323 and interworked calls, a SIP equivalent response code.
Src-ip	Source IP address (the IP address of the device attempting to establish communications). This can be an IPv4 address or an IPv6 address.
Dst-ip	Destination IP address (the IP address of the destination for a communication attempt). The destination IP is recorded in the same format as Src-ip.
Src-port	Source port: the IP port of the device attempting to establish communications.
Dst-port	Destination port: the IP port of the destination for a communication attempt.
Src-alias	If present, the first H.323 alias associated with the originator of the message. If present, the first E.164 alias associated with the originator of the message.
Dst-alias	If present, the first H.323 alias associated with the recipient of the message. If present, the first E.164 alias associated with the recipient of the message.
Detail	Descriptive detail of the Event.
Auth	Whether the call attempt has been authenticated successfully.
Method	SIP method (INVITE, BYE, UPDATE, REGISTER, SUBSCRIBE, etc).
Contact	Contact: header from REGISTER.
AOR	Address of record.
Call-id	The Call-ID header field uniquely identifies a particular invitation or all registrations of a particular client.
Call-serial-number	The local Call Serial Number that is common to all protocol messages for a particular call.
Tag	The Tag is common to all searches and protocol messages across a Cisco VCS network for all forks of a call.
Call-routed	Indicates if the Cisco 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.

Name	Description
Time	A full UTC timestamp in YYYY/MM/DD-HH:MM:SS format. Using this format permits simple ASCII text sorting/ordering to naturally sort by time. This is included due to the limitations of standard syslog timestamps.
Level	The level of the event as defined in the About Event Log levels section.
UTCTime	Time the event occurred, shown in UTC format.

Events and levels

The following table lists the events that can appear in the Event Log.

Event	Description	Level
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 Cisco VCS application has been exited. Further information may be provided in the **Detail** event parameter.	1
Application Failed	The Cisco VCS application is out of service due to an unexpected failure.	1
Application Start	The Cisco VCS has started. Further detail may be provided in the **Detail** event parameter.	1
Application Warning	The Cisco 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

Event	Description	Level
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 Cisco VCS has **Call Routed mode** set to *Optimal* and has removed itself from the call signaling path.	1
Completed System Backup	A system backup has completed.	1
Completed System restore	A system restore has completed.	1
Configlog Cleared	An operator cleared the Configuration Log.	1
Decode Error	A syntax error was encountered when decoding a SIP or H.323 message.	1
Directory Service Database Started	The TMS Agent database has started.	1
Directory Service Database Stopped	The TMS Agent database has stopped.	1
Directory Service Failed Restarting	The TMS Agent failed to restart.	1
Directory Service Restarted	The TMS Agent has restarted.	1
Directory Service Restarting	The TMS Agent is restarting.	1
Directory Service Starting	The TMS Agent is starting.	1

Event	Description	Level
Directory Service Shutting Down	The TMS Agent is shutting down.	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
FindMe Transfer	FindMe user accounts have been migrated across clusters. The **Detail** event parameter provides additional details.	1
Hardware Failure	There is an issue with the Cisco 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
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 Cisco 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 Cisco VCS. ▪ Clustering is enabled but bandwidth across the cluster has not been configured identically, and the Cisco VCS has received a message relating to an unknown peer, link, pipe, subzone or zone.	1

Event	Description	Level
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 Cisco VCS is unable to communicate with another system over TLS. Refer to the event parameters for more information.	1
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. Refer to the **Reason** event parameter for specific information.	1
Registration Accepted	A registration request has been accepted.	1
Registration Refresh Accepted	A request to refresh or keep a registration alive has been accepted.	3
Registration Refresh Rejected	A request to refresh a registration has been rejected.	1
Registration Refresh Requested	A request to refresh or keep a registration alive has been received.	3
Registration Rejected	A registration request has been rejected. The **Reason** and **Detail** event parameters provide more information about the nature of the rejection.	1
Registration Removed	A registration has been removed by the Cisco 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

Event	Description	Level
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. Refer to the **Reason** event parameter for 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 Cisco VCS is in **Call loop detection** mode and has identified and terminated a looped branch of a search.	2
Secure mode disabled	The Cisco VCS has successfully exited **Advanced account security** mode.	1
Secure mode enabled	The Cisco VCS has successfully entered **Advanced account security** mode.	1
Security Alert	A potential security-related attack on the Cisco 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

Event	Description	Level
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
TLS Negotiation Error	Transport Layer Security (TLS) connection failed to negotiate.	1
TMS Agent backup completed	The TMS Agent backup process has completed.	1
TMS Agent backup error	An error occurred while attempting a TMS Agent backup.	1

Event	Description	Level
TMS Agent backup started	The TMS Agent backup process has started.	1
TMS Agent restore completed	The TMS Agent restore process has completed.	1
TMS Agent Restore error	An error occurred while attempting a TMS Agent restore.	1
TMS Agent restore started	The TMS Agent restore process has started.	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. Refer to the **Detail** event parameter for 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
Warning acknowledged	An administrator has acknowledged a warning. The **Detail** event parameter provides information about the nature of the issue.	1
Warning lowered	The issue that caused a warning to be raised has been resolved. The **Detail** event parameter provides information about the nature of the issue.	1
Warning raised	The Cisco VCS has detected an issue and raised a warning. The **Detail** event parameter provides information about the nature of the issue.	1

CPL reference

Call Processing Language (CPL) is an XML-based language for defining call handling. This section gives details of the Cisco VCS's implementation of the CPL language and should be read in conjunction with the CPL standard *RFC 3880* [5] and the *Guide to writing CPL* [22].

The Cisco VCS has many powerful inbuilt transform features so CPL should be required only if advanced call handling rules are required.

The Cisco 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 Cisco 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 Cisco 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>
```

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 Cisco 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 Cisco 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.	

Field parameter attributes	SIP	H.323
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 Cisco 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 Cisco 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.

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 Cisco 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	Cisco 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 Cisco 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 Cisco 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 Cisco 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
- Change of domain name
- 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

In this example, only calls from users with authenticated source addresses are allowed. See About device authentication for details on how to enable authentication.

```
<?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

In this example, user **ceo** will only accept calls from users **vpsales**, **vpmarketing** or **vpengineering**.

```
<?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

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.

```
<?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: change of domain name

In this example, **Example Inc** has changed its domain from **example.net** to **example.com**. For a period of time some users are still registered at **example.net**. The following script would attempt to connect calls to **user@example.com** first and if that fails then fallback to **example.net**.

```
<?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="(.*)@example.com">
                <proxy>
                    <failure>
                        <!-- Failed to contact using example.com, retry the request
                        with example.net -->
                        <taa:location clear="yes" regex="(.*)@example.com"
                        replace="\1@example.net">
                            <proxy/>
                        </taa:location>
                    </failure>
                </proxy>
            </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
                Cisco VCS"/>
            </not-present>
        </address-switch>
    </taa:routed>
</cpl>
```

CPL example: block calls from Default Zone and Default Subzone

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

In these examples, a gateway is registered to the Cisco 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* [5] for details).

The Cisco 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 Cisco 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 configuration for device authentication

The Cisco VCS can be configured to use a database on an LDAP Directory Server to store device authentication credential information (usernames, passwords, and other relevant information).

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 Cisco 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 in **ldif** format from the web interface on the Cisco VCS. To do this:

1. Go to **VCS configuration > Authentication > Devices > LDAP 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 step-by-step 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 a command prompt and 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 Cisco 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 *Alias origin* in the Device authentication using LDAP section.

Securing with TLS

To enable Active Directory to use TLS, you must request and install a certificate on the Active Directory server. The certificate must meet the following requirements:

- Be located in the Local Computer’s Personal certificate store. This can be seen using the **Certificates** MMC snap-in.
- Have the private details on how to obtain a key associated for use with it stored locally. When viewing the certificate you should see a message saying “You have a private key that corresponds to this certificate’’.
- Have a private key that does not have strong private key protection enabled. This is an attribute that can be added to a key request.
- The Enhanced Key Usage extension includes the Server Authentication object identifier, again this forms part of the key request.
- Issued by a CA that both the domain controller and the client trust.
- Include the Active Directory fully qualified domain name of the domain controller in the common name in the subject field and/or the DNS entry in the subject alternative name extension.

To configure the Cisco 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 Cisco VCS by navigating to **Maintenance > Security certificates**.

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. Copy the OpenLDAP files to the OpenLDAP schema directory:

   /etc/openldap/schemas/commobject.ldif

   /etc/openldap/schemas/h323identity.ldif

   /etc/openldap/schemas/h235identity.ldif

   /etc/openldap/schemas/sipidentity.ldif

2. Edit **/etc/openldap/slapd.conf** to add the new schemas. You need to add the following lines:

   include /etc/openldap/schemas/commobject.ldif

   include /etc/openldap/schemas/h323identity.ldif

   include /etc/openldap/schemas/h235identity.ldif

   include /etc/openldap/schemas/sipidentity.ldif

The OpenLDAP daemon (**slapd**) must be restarted for the new schemas to take effect.

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 using the command:

   ```
   slapadd -l <ldif_file>
   ```

This organizational unit will form the BaseDN to which the Cisco 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 Cisco 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 using the command:

   ```
   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 *Alias origin* in the Device authentication using LDAP section.

Securing with TLS

The connection to the LDAP server can be encrypted by enabling Transport Level Security (TLS) on the connection. To do this you must create an X.509 certificate for the LDAP server to allow the Cisco

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 Cisco 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 Cisco VCS by navigating to: **Maintenance > Security certificates**.

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* [3]
Weight	is the weight as defined by *RFC 2782* [3]
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* [6].

Changing the default SSH key

Default SSH key warnings

A warning message "Security alert: the SSH service is using the default key" is displayed if your Cisco VCS is still configured with its factory default SSH key.

Using the default key means that SSH sessions established to the Cisco VCS may be vulnerable to "man-in-the-middle" attacks, so you are recommended to generate new SSH keys which are unique to your Cisco VCS.

Standalone Cisco VCS

Use the following instructions to generate a new SSH key for the Cisco VCS, entering all commands from the CLI while logged in as *root*:

1. Type **regeneratesshkey**.
2. Type **exit** to log out of the root account.

Clustered Cisco VCS

Use the following instructions to generate new SSH keys for each cluster peer.

Enter the following commands from the CLI while logged in as *root*:

1. On each Cisco VCS peer in turn:
   a. Type **cluster**.
   b. Select option *(3)* to temporarily disable replication on each Cisco VCS.
      Follow the instructions but DO NOT remove the Cisco VCS from the list of peers.
   c. Select *(q)* to quit.
2. On each Cisco VCS peer in turn:
   a. Type **regeneratesshkey**.
3. After each Cisco VCS has had replication disabled and its SSH key regenerated, on each Cisco VCS peer in turn:
   a. Type **cluster**.
      - On the master Cisco VCS, select option *(1)* and follow the instructions to set it as the replication master.
      - On each non-master Cisco VCS, select option *(2)* and follow the instructions to set it to replicate with a peer.
   b. Select **(q)** to quit.
4. On every Cisco VCS in turn:
   a. Type **cluster**.
   b. Select option **(5)** to check that Cisco VCS replication is working correctly.
   c. Select **(q)** to quit.
5. Type **exit** to log out of the root account.

Finally, you must restart every Cisco VCS. You are recommended to do this from the web interface:

6. Go to **Maintenance > Restart**.
   You are taken to the **Restart** page.
7. Check the number of calls and registrations currently in place.
8. Click **Restart system** and then confirm the restart when asked.

When you next log in to the Cisco VCS over SSH you may receive a warning that the key identity of the Cisco VCS has changed. Please follow the appropriate process for your SSH client to suppress this warning.

If your Cisco VCS is subsequently downgraded to an earlier version of Cisco VCS firmware, the default SSH keys will be restored.

Restoring default configuration

It is possible to restore the Cisco VCS to its default configuration. This is done through the CLI using **xCommand DefaultValuesSet**. This command is not available through the web interface.

The DefaultValuesSet command allows you to specify the level of configuration to restore, from 1 to 3 as follows:

- **Level 1**: resets most configuration items to their default value, with the exception of the Level 2 and Level 3 items shown in the tables below.
- **Level 2**: resets configuration items mostly related to remote authentication (listed in Configuration items reset by DefaultValuesSet level 2), plus Level 1 items to their default values.
- **Level 3**: resets all critical configuration items (listed in Configuration items reset by DefaultValuesSet level 3 below) plus Level 1 and Level 2 items to their default values.

See the Cisco VCS Command Reference [40] for a full list of all configuration items and where applicable their default values.

Note:xCommand DefaultValuesSet Level: 3 must be used with caution, as it resets the system's IPv4 and IPv6 addresses, meaning you will no longer be able to access the system over IP. It also deletes all option keys including pre-installed options such as Expressway and the number of calls. It also deletes all links configured on the Cisco VCS, including the automatically configured default links between the Default Subzone, Traversal Subzone and Default Zone. Without these links, calls will not be able to be placed. To restore these links, you should run the command **xCommand DefaultLinksAdd** after **xCommand DefaultValuesSet Level: 3**. These links can also be restored manually using the web interface - see the Default links section for more information.

Configuration items reset by DefaultValuesSet level 3

The following table lists the configuration items that are reset by **xCommand DefaultValuesSet Level: 3** and their reset values.

Configuration item	Reset value
Administration HTTP Mode	On
Administration HTTPS Mode	On
Administration SSH Mode	On
Administration Telnet Mode	Off
Ethernet [1..2] IP V4 Address	192.168.0.100

Configuration item	Reset value
Ethernet [1..2] IP V4 StaticNAT Address	<blank>
Ethernet [1..2] IP V4 StaticNAT Mode	Off
Ethernet [1..2] IP V4 SubnetMask	255.255.255.0
Ethernet [1..2] IP V6 Address	<blank>
Ethernet [1..2] Speed	Auto
IPProtocol	IPv4
IP DNS Domain Name	<blank>
IP DNS Hostname	<blank>
IP DNS Server [1..5] Address	<blank>
IP Gateway	127.0.0.1
IP Route [1..50] Address	<blank>
IP Route [1..50] Gateway	<blank>
IP Route [1..50] Interface	Auto
IP Route [1..50] PrefixLength	32
IP V6 Gateway	<blank>
NTP Address	<blank>
Option [1..64] Key	<all option keys are deleted>
SystemUnit AdminAccount [1..15] Access	ReadWrite
SystemUnit AdminAccount [1..15] Name	<blank>
SystemUnit AdminAccount [1..15] Password	<blank>
SystemUnit Maintenance Mode	Off
SystemUnit Name	<blank>
SystemUnit Password	TANDBERG
SystemUnit StrictPassword Enforce	Off

Configuration items reset by DefaultValuesSet level 2

The following table lists the configuration items that are reset by **xCommand DefaultValuesSet Level: 2** and their reset values.

Configuration item	Reset value
Alternates Cluster Name	<blank>

Configuration item	Reset value
Authentication ADS ADDomain	<blank>
Authentication ADS Clockskew	300
Authentication ADS DC Address	<blank>
Authentication ADS Encryption	TLS
Authentication ADS KDC Address	<blank>
Authentication ADS KDC Port	88
Authentication ADS Mode	Off
Authentication ADS SecureChannel	Auto
Authentication ADS SPNEGO	Enabled
Authentication ADS Workgroup	<blank>
Login Administrator Groups Group [1..30] Access	ReadWrite
Login Administrator Groups Group [1..30] Name	<blank>
Login Administrator Source	Local
Login Remote LDAP BaseDN Accounts	<blank>
Login Remote LDAP BaseDN Groups	<blank>
Login Remote LDAP DirectoryType	ActiveDirectory
Login Remote LDAP Encryption	Off
Login Remote LDAP SASL	DIGEST-MD5
Login Remote LDAP Server Address	<blank>
Login Remote LDAP Server Port	389
Login Remote LDAP VCS BindDN	<blank>
Login Remote LDAP VCS BindPassword	<blank>
Login Remote LDAP VCS BindUsername	<blank>
Login Remote Protocol	LDAP
Login User Groups Group [1..15] Access	ReadWrite
Login User Groups Group [1..15] Name	<blank>
Login User Source	Local

Password encryption

All passwords configured on the Cisco VCS are stored in encrypted form. This applies to the following, 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 Cisco VCS)
- outbound connection credentials (used by the Cisco VCS when required to authenticate with another system)
- LDAP server (used by the Cisco VCS when binding to an LDAP server)

Passwords can be configured using either the CLI or the web interface.

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 will type the password in plain text. However, after the command has been executed, the password will be displayed in its encrypted form with a **{cipher}** prefix, for example:

xConfiguration LDAP Password: "{cipher}xcy6k+4NgB025vYEgoEXXw=="

Note: FindMe is a standalone application that can be hosted by the Cisco VCS or by another remote server. This means that FindMe user account information is not configured or accessible using the CLI of the Cisco VCS. However, FindMe user passwords are still stored securely.

Maximum length of passwords

When a password is encrypted, it uses more characters than the original plain text version of the password. For each type of password, the maximum number of plain text characters that can be entered and the maximum number of encrypted characters that are displayed through the CLI are shown in the table below.

Password type	Maximum plain text characters	Maximum displayed encrypted characters
Admin account	16	65
Administrator accounts	16	65
Local Database authentication credentials	128	215
Outbound connection credentials	128	215
LDAP server	60	122
FindMe accounts	30	82

Pattern matching variables

The Cisco 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 Cisco 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 currently configured on the Cisco VCS.	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.	not applicable
%ipv4_1%	xConfiguration Ethernet 1 IP V4 Address	Matches the IPv4 address currently configured for LAN 1.	Replaces the string with the LAN 1 IPv4 address.
%ipv4_2%	xConfiguration Ethernet 2 IP V4 Address	Matches the IPv4 address currently configured for LAN 2.	Replaces the string with the LAN 2 IPv4 address.
%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.	not applicable
%ipv6_1%	xConfiguration Ethernet 1 IP V6 Address	Matches the IPv6 address currently configured for LAN 1.	Replaces the string with the LAN 1 IPv6 address.

String	Represents value returned by...	When used in a Pattern field	When used in a Replace field
%ipv6_2%	xConfiguration Ethernet 2 IP V6 Address	Matches the IPv6 address currently configured for LAN 2.	Replaces the string with the LAN 2 IPv6 address.
%localdomains%	xConfiguration SIP Domains Domain 1 Name ... xConfiguration SIP Domains Domain 20 Name	Matches all the SIP domains currently configured on the Cisco VCS.	not applicable
%localdomain1% ... %localdomain20%	xConfiguration SIP Domains Domain 1 Name ... xConfiguration SIP Domains Domain 20 Name	Matches the specified SIP domain. Up to 20 SIP domains can be configured on the Cisco VCS, and they are identified by an index number between 1 and 20.	Replaces the string with the specified SIP domain.
%systemname%	xConfiguration SystemUnit Name	Matches the Cisco VCS's System Name.	Replaces the string with the Cisco 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

The Cisco VCS uses different IP ports and protocols for different services and functions, and many of these are configurable. The table below lists each of these services and functions. For each, it shows the default port(s) and protocol used and whether these ports are used for inbound or outbound communications. If the ports are configurable it shows the available range and how to configure them using the web interface or CLI.

The information in the table below shows all possible services and the generic defaults for each. The actual services and ports used on your system will vary depending on its configuration, the option keys installed and features that have been enabled. A specific list of all the IP ports in use on a particular Cisco VCS can be viewed via the port usage pages.

Note: two services or functions cannot share the same port and protocol; if you attempt to change an existing port or range and it conflicts with another service, you will get a warning message.

Service/ function	Description	Default	Direction	Available range	Configurable via
SSH and FindMe replication for clusters	Used for encrypted command line administration. Also used to replicate FindMe data if the Cisco VCS is part of a cluster with FindMe enabled.	22 TCP	inbound	not configurable	
Telnet	Used for unencrypted command line administration.	23 TCP	inbound	not configurable	
HTTP	Used for unencrypted web administration.	80 TCP	inbound	not configurable	
NTP	Used for updating the system time (and important for H.235 security).	123 UDP	outbound	not configurable	
SNMP	Used for network management.	161 UDP	inbound	not configurable	
TMS Agent	Used for diagnostics.	389 TCP	inbound	not configurable	
HTTPS	Used for encrypted web administration. Also used to replicate FindMe data if the Cisco VCS is part of a cluster with FindMe enabled.	443 TCP	inbound	not configurable	

Service/ function	Description	Default	Direction	Available range	Configurable via
Reserved for future use		636	inbound	not configurable	
Gatekeeper discovery	Used for multicast gatekeeper discovery. Note that the Cisco VCS does not listen on this port when **H.323 Gatekeeper Auto discover mode** is set to *Off* (this has the effect of disabling IGMP messages).	1718 UDP	inbound	not configurable	
Clustering	Used for communication between cluster peers	4369-4380 TCP	inbound outbound	not configurable	
Clustering	Used to recover from intra-cluster communication failure	4371 UDP	inbound	not configurable	
Clustering	Used for IPsec secure communication between cluster peers.	500 UDP	inbound	not configurable	
H.323 registration Clustering	Listens for inbound H.323 UDP registrations. If the Cisco VCS is part of a cluster, this port is also used for inbound and outbound communication with peers, even if H.323 is disabled.	1719 UDP	inbound outbound	1024 - 65534	**VCS configuration > Protocols > H.323** **xConfiguration H323 Gatekeeper Registration UDP Port**
H.323 call signaling	Listens for H.323 call signaling.	1720 TCP	inbound	1024 - 65534	**VCS configuration > Protocols > H.323** **xConfiguration H323 Gatekeeper CallSignaling TCP Port**
Traversal server media demultiplexing RTP	Used on the Cisco VCS Expressway for demultiplexing RTP media.	2776 UDP	inbound outbound	1024 - 65534	**VCS configuration > Expressway > Ports** **xConfiguration Traversal Server Media Demultiplexing RTP Port**

Service/ function	Description	Default	Direction	Available range	Configurable via
Assent call signaling	Used on the Cisco VCS Expressway for Assent signaling.	2776 TCP	inbound	1024 - 65534	**VCS configuration > Expressway > Ports** **xConfiguration Traversal Server H323 Assent CallSignaling Port**
H.460.18 call signaling	Used on the Cisco VCS Expressway for H.460.18 signaling.	2777 TCP	inbound	1024 - 65534	**VCS configuration > Expressway > Ports** **xConfiguration Traversal Server H323 H46018 CallSignaling Port**
Traversal server media demultiplexing RTCP	Used on the Cisco VCS Expressway for demultiplexing RTCP media.	2777 UDP	inbound outbound	1024 - 65534	**VCS configuration > Expressway > Ports** **xConfiguration Traversal Server Media Demultiplexing RTCP Port**
TURN services	Cisco VCS Expressway listening port for TURN relay requests.	3478 UDP	inbound	1024 - 65534	**VCS configuration > Expressway > TURN** **xConfiguration Traversal Server TURN Port**
VCS database and TMS Agent (for clusters or Cisco TMS)	Encrypted administration connector to the VCS database. Used if the Cisco VCS is part of a cluster with FindMe or Device Provisioning enabled, or if the Cisco VCS is managed through Cisco TMS.	4444 TCP	inbound	not configurable	
SIP UDP	Listens for incoming SIP UDP calls.	5060 UDP	inbound outbound	1024 - 65534	**VCS configuration > Protocols > SIP > Configuration** **xConfiguration SIP UDP Port**
SIP TCP	Listens for incoming SIP TCP calls.	5060 TCP	inbound	1024 - 65534	**VCS configuration > Protocols > SIP > Configuration** **xConfiguration SIP TCP Port**

Service/ function	Description	Default	Direction	Available range	Configurable via
SIP TLS	Listens for incoming SIP TLS calls.	6061 TCP	inbound	1024 - 65534	**VCS configuration > Protocols > SIP > Configuration** **xConfiguration SIP TLS Port**
Traversal server zone H323 Port	The port on the Cisco VCS Expressway being used for H.323 firewall traversal from a particular traversal client.	6001 UDP, increments by 1 for each new zone	inbound	1024 - 65534	**VCS configuration > Zones > Edit zone** **xConfiguration Zones Zone [1..1000] TraversalServer H323 Port**
Traversal server zone SIP Port	The port on the Cisco VCS Expressway being used for SIP firewall traversal from a particular traversal client.	7001 TCP, increments by 1 for each new zone	inbound	1024 - 65534	**VCS configuration > Zones > Edit zone** **xConfiguration Zones Zone [1..1000] TraversalServer SIP Port**
TMS Agent	Used for Device Provisioning and FindMe.	8989 TCP	inbound	not configurable	
DNS	Used for sending requests to DNS servers.	10000 - 10210 UDP	outbound	not configurable	
H.225 and H.245 call signaling port range	The range of ports to be used for call signalling after a call is established.	15000 - 19999 TCP	inbound outbound	1024 - 65534	**VCS configuration > Protocols > H.323** **xConfiguration H323 Gatekeeper CallSignaling PortRange Start** **xConfiguration H323 Gatekeeper CallSignaling PortRange End**
SIP TCP outbound port range	The range of ports to be used by outbound TCP/TLS SIP connections to a remote SIP device.	25000 - 29999 TCP	outbound	1024 - 65534	**VCS configuration > Protocols > SIP > Configuration** **xConfiguration SIP TCP Outbound Port Start** **xConfiguration SIP TCP Outbound Port End**

Service/ function	Description	Default	Direction	Available range	Configurable via
Traversal media port range	For traversal calls (where the Cisco VCS takes the media as well as the signaling), the range of ports to be used for the media. Ports are allocated from this range in pairs, with the first port number of each pair being an even number. See About the Traversal Subzone for more information.	50000 - 52399 UDP	outbound	1024 - 65533	**VCS configuration > Local Zone > Traversal Subzone** **xConfiguration Traversal Media Port Start** **xConfiguration Traversal Media Port End**
TURN relay media port range	The range of ports available for TURN media relay.	60000 - 61200 UDP	inbound outbound	1024 - 65534	**VCS configuration > Expressway > TURN** **xConfiguration Traversal Server TURN Media Port Start** **xConfiguration Traversal Server TURN Media Port End**
LDAP	Used for outbound connection to an LDAP server (if the Cisco VCS is configured to use an LDAP server for H.350 authentication).	uses a TCP source port from the ephemeral range			
External manager	Used for outbound connection to an external manager, for example Cisco TMS.	uses a TCP source port from the ephemeral range			
Third-party FindMe / User Policy server	Used for outbound connection to a third-party FindMe / User Policy server.	uses a TCP source port from the ephemeral range			
Remote logging	Used to send messages to the remote syslog server.	uses a TCP source port from the ephemeral range			
TMS Agent	Used to connect to another Cisco VCS or Cisco TMS for data replication.	uses a TCP source port from the ephemeral range			

Service/ function	Description	Default	Direction	Available range	Configurable via
Login authentication	Used to connect to an LDAP server for login account authentication.	uses a TCP source port from the ephemeral range			
Active Directory Service and Kerberos	Used to connect to an ADS Domain Controller and a Kerberos Key Distribution Center for account authentication.	uses TCP source ports from the ephemeral range			

Note that the range of ephemeral ports can be configured by using the CLI commands **xConfiguration IP Ephemeral PortRange Start** and **xConfiguration IP Ephemeral PortRange End**.

Regular expressions

Regular expressions can be used in conjunction with a number of Cisco VCS features such as alias transformations, zone transformations, CPL policy and ENUM. The Cisco 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 *Mastering Regular Expressions* [9].

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$** matches any string that is exactly 3 digits long.
(?!...)	Negative lookahead. Defines a subexpression that must not be present in order for there to be a match.	**(?!.*@example.com$).*** matches any string that does not end with **@example.com**.
(?<!...)	Negative lookbehind. Defines a subexpression that must not be present in order for there to be a match.	**.*(?<!.*@example.com$)** matches any string that does not end with **@example.com**.

Note that regex comparisons are not case sensitive.

For an example of regular expression usage, see the CPL examples section.

Supported characters

The Cisco 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 have different restrictions and these are noted in the relevant sections of this guide, including:

- Administrator and user groups

Case sensitivity

Text items entered through the CLI and web interface are case insensitive. The only exception is passwords which are case sensitive.

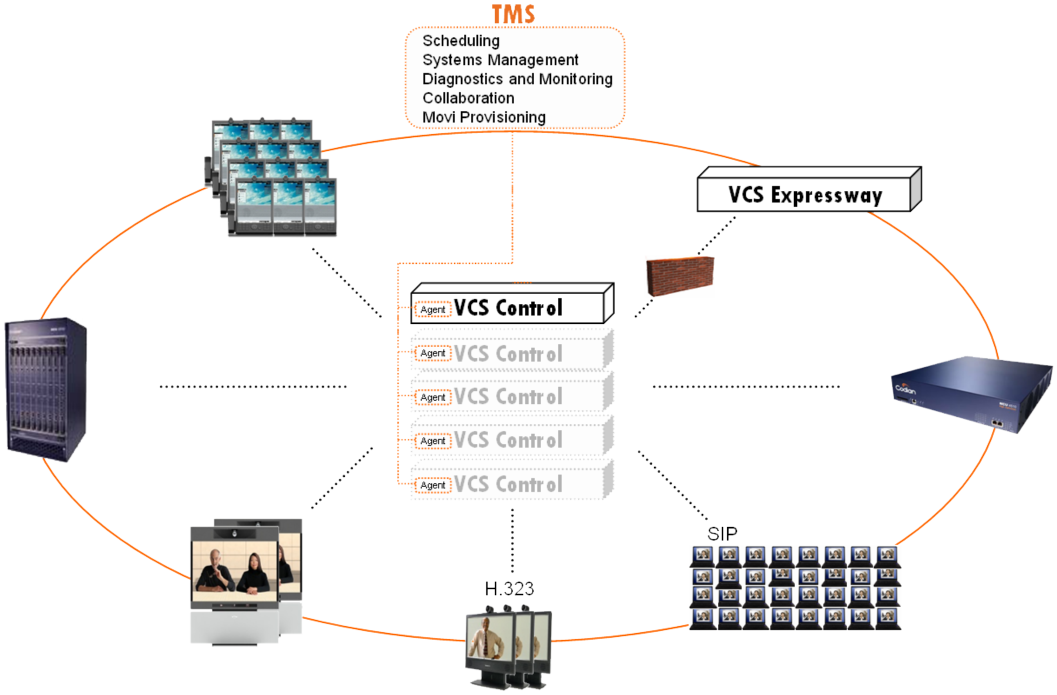
TMS Agent

The TMS Agent is a process that runs on the Cisco VCS to manage FindMe and Device Provisioning data.

It acts on behalf of Cisco TMS so that Cisco TMS is not a single point of failure, and enables each Cisco VCS to share the load. It supports the replication of FindMe and provisioning data, sharing the data among cluster peers as well as the central Cisco TMS, providing resilience in case of connection failures between any Cisco VCS and Cisco TMS.

TMS Agent is installed as part of the **VCS platform** and requires no configuration on the Cisco VCS, other than ensuring the default password is changed (see **TMS Agent account passwords** below).

- You must use Cisco TMS to create and manage Device Provisioning data.
- FindMe accounts may be set up using Cisco TMS or Cisco VCS.



FindMe

The TMS Agent replicates changes to FindMe account information across peers in a Cisco VCS cluster (FindMe account changes can be made on any peer, not just the master), across to Cisco TMS and also across to other Cisco VCS clusters managed by the same Cisco TMS.

Note that the FindMe option key must be installed on the Cisco VCS.

Device Provisioning

The TMS Agent works with the TMS Provisioning Directory to replicate and distribute the provisioning information and phonebook from Cisco TMS via Cisco VCSs to endpoint devices. Cisco VCSs cache and replicate data among themselves in case connection to Cisco TMS is lost.

Note that the Device Provisioning option key must be installed on the Cisco VCS.

TMS Agent account passwords

TMS agent is accessed via two accounts: one for connecting via LDAP into the TMS Agent database, and one for managing the replication of the TMS Agent database. These accounts are only used by the internal processes running on the Cisco VCS and Cisco TMS. System administrators must not use these accounts.

These accounts have a **username** of **cn=Directory Manager** and a default **password** of **TANDBERG** (all upper case). Both passwords must be changed as soon as possible to maintain security of the Cisco VCS data. Warnings are shown on the web UI and the CLI if either account has the default password set.

- If your Cisco VCS uses Cisco TMS as an external manager, you must use Cisco TMS to change the passwords on these accounts.
- If your Cisco VCS is not managed by Cisco TMS, you have to change these passwords by logging into the Cisco VCS as the root user. Note that if your Cisco VCS is subsequently reconfigured to use Cisco TMS, the password must first be reset to the default value of TANDBERG.

See the TMS Agent passwords section for full instructions on changing passwords.

TMS Agent passwords

This section contains instructions for changing passwords on the TMS Agent.

TMS Agent LDAP and replication accounts

The TMS Agent is accessed via two accounts: one for connecting via LDAP into the TMS Agent database, and one for managing the replication of the TMS Agent database. These accounts have a username of **cn=Directory Manager** and a default password of **TANDBERG** (all upper case). For security reasons you must change these accounts' passwords from their default values as soon as possible. You will receive a warning on the Cisco VCS web UI and the CLI if either account has the default password configured.

Note: these accounts are only used by the internal processes running on the Cisco VCS and Cisco TMS. System administrators must not use these accounts.

Cisco VCSs managed by Cisco TMS

If your Cisco VCS uses Cisco TMS as an external manager, you must use Cisco TMS to change the passwords on these accounts. This ensures that the Cisco VCS and Cisco TMS keep in sync with each other. If your Cisco VCS is part of a cluster, Cisco TMS will replicate the modified password across all peers.

To change the TMS Agent LDAP account password from within Cisco TMS:

1. Go to **Administrative Tools > Configuration > TMS Agent Settings**.
2. Enter the new **LDAP Configuration Password**.
3. Click **Save**.

To change the TMS Agent replication account password from within Cisco TMS:

1. Go to **Administrative Tools > Configuration > TMS Agent Settings**.
2. Enter the new **LDAP Replication Password**.
3. Click **Save**.

These instructions are for Cisco TMS version 12.5. Refer to the Cisco TMS documentation for later releases.

Cisco VCSs not managed by Cisco TMS

If your Cisco VCS is not managed by Cisco TMS, you have to change these passwords by logging into the Cisco VCS as the root user (by default you can only do this using a serial connection or SSH).

To change the password for the TMS Agent LDAP account:

1. From the CLI, logged in as root, type **tmsagent_ldap_passwd**.
   You are asked for the new password.
2. Enter the new password and, when prompted, retype the password.
3. Type **exit** to log out of the root account.

To change the password for the TMS Agent replication account:

1. From the CLI, logged in as root, type **tmsagent_replication_passwd**.
   You are asked for the new password.
2. Enter the new password and, when prompted, retype the password.
3. Type **exit** to log out of the root account.

Note: if your Cisco VCS is subsequently reconfigured to use Cisco TMS, the password must first be reset to the default value of TANDBERG.

What are traversal calls?

A traversal call is any call passing through the Cisco 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 Cisco VCS but the media goes directly between the endpoints (or between one endpoint and another Cisco VCS in the call route, or between two Cisco VCSs in the call route).

- A call is “traversal” or “non-traversal” from the point of view of the Cisco VCS through which it is being routed at the time. A call between two endpoints may pass through two or more Cisco VCSs. Some of these Cisco VCSs may just take the signaling, in which case the call will be a non-traversal call for that Cisco VCS. Other Cisco 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 Cisco VCS.

The following types of calls require the Cisco VCS to take the media. They are classified as traversal calls and will always pass through the Traversal Subzone:

- firewall traversal calls, where the local Cisco VCS is either the traversal client or traversal server
- calls that are gatewayed (interworked) between H.323 and SIP on the local Cisco VCS
- calls that are gatewayed (interworked) between IPv4 and IPv6 on the local Cisco VCS
- for Cisco VCSs with Dual Network Interfaces 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)
- encrypted calls to and from Microsoft OCS Server 2007 (requires the *Enhanced OCS Collaboration* option key)

All such calls require a traversal call license each time they pass through the Traversal Subzone.

Traversal calls use more resource than non-traversal calls, and the numbers of each type of call are licensed separately. The Cisco 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 Cisco VCS by purchasing and installing the appropriate option key.

Note that a non-traversal call on a Cisco VCS Expressway will consume a traversal license if there are no non-traversal call licenses available.

Warnings list

Warnings occur when an event or configuration change has taken place on the Cisco VCS that requires some manual administrator intervention, such as a restart. Warnings may also be raised for hardware and environmental issues such as faulty disks and fans or high temperatures.

The **Warnings** page (**Status > Warnings**) provides a list of all the warnings currently in place on your system (and, where applicable, their proposed resolution). When there are unacknowledged warnings in place on the Cisco VCS, a warning icon ⚠ appears at the top right of all pages.

The following table lists the warnings that can be raised on the Cisco VCS.

ID	Warning message	Resolution
10001	Configuration warning: expected default link between the Default Subzone and the Traversal Subzone is missing	Configure default links
10002	Configuration warning: expected default link between the Default Subzone and the Default Zone is missing	Configure default links
10003	Configuration warning: expected default link between the Default Subzone and the Cluster Subzone is missing	Configure default links
10004	Configuration warning: expected default link between the Traversal Subzone and the Default Zone is missing	Configure default links
10005	Port conflict: one or more ports have been configured for use by more than one service	Review the port configuration
10006	Configuration warning: IP protocol is set to both IPv4 and IPv6, but the VCS does not have any IPv6 addresses defined	Configure IP settings
10007	Configuration warning: IP protocol is set to both IPv4 and IPv6, but the VCS does not have any IPv4 addresses defined	Configure IP settings
10008	Configuration warning: IP protocol is set to both IPv4 and IPv6, but the VCS does not have an IPv4 gateway defined	Configure IP settings
10009	Configuration warning: IP protocol is set to both IPv4 and IPv6, but the VCS does not have an IPv6 gateway defined	Configure IP settings
10010	Restart required: Ethernet configuration has been changed, however a restart is required for this to take effect	Restart the VCS
10011	Restart required: HTTP service has been changed, however a restart is required for this to take effect	Restart the VCS
10012	Restart required: HTTPS service has been changed, however a restart is required for this to take effect	Restart the VCS
10013	Restart required: IP configuration has been changed, however a restart is required for this to take effect	Restart the VCS
10014	Restart required: port configuration has been changed, however a restart is required for this to take effect	Restart the VCS
10015	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

ID	Warning message	Resolution
10016	Configuration conflict: H323-SIP Protocol Interworking mode is set to "Registered only" but the H323-SIP Interworking Gateway option key has been deleted	Reconfigure Interworking mode or reinstall the option key
10017	Restart required: SNMP service has been changed, however a restart is required for this to take effect	Restart the VCS
10018	Restart required: SSH service has been changed, however a restart is required for this to take effect	Restart the VCS
10019	Restart required: Telnet service has been changed, however a restart is required for this to take effect	Restart the VCS
10020	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
10021	Restart required: the Dual Network Interfaces option key has been changed, however a restart is required for this to take effect	Restart the VCS
10022	Capacity warning: the number of concurrent traversal calls has approached the licensed limit	Contact your Cisco representative
10023	Capacity warning: the number of concurrent non-traversal calls has approached the licensed limit	Contact your Cisco representative
10024	Capacity warning: the number of concurrent Registrations has approached the licensed limit	Contact your Cisco representative
10025	Configuration conflict: a domain is in use by the OCS Relay application that has not been configured on the VCS	Reconfigure the OCS Relay or view and edit the VCS SIP domains
10026	Security alert: the admin user has the default password set	Change the admin password
10027	Security alert: the root user has the default password set	Change the root password
10028	Security alert: the TMS Agent database has the default LDAP password set	Change the TMS Agent LDAP password
10029	Security alert: the TMS Agent database has the default replication password set	Change the TMS Agent replication password
10030	Security alert: the SSH service is using the default key	Replace the default SSH key
10031	Security alert: one or more administrators has a password that does not meet strictness requirements	View and edit administrator accounts
10032	Cluster replication error: NTP server is not configured	Configure an NTP server
10033	Cluster replication error: the NTP server is unreachable	Reconfigure the NTP server

ID	Warning message	Resolution
10034	Cluster replication error: configuration master ID is inconsistent, manual synchronization of configuration is required	View cluster replication troubleshooting instructions
10035	Cluster replication error: cannot find master or this peer's configuration file, manual synchronization of configuration is required	View cluster replication troubleshooting instructions
10036	Cluster replication error: this peer's configuration conflicts with the master's configuration, manual synchronization of configuration is required	View cluster replication troubleshooting instructions
10037	Cluster replication error: the Master peer is unreachable	Check the list of peers for this cluster
10038	Cluster replication error: the local VCS does not appear in the list of peers	Check the list of peers for this cluster
10039	Cluster replication error: there was an error during automatic replication of configuration	View cluster replication troubleshooting instructions
10040	Cluster replication error: automatic replication of configuration has been temporarily disabled because an upgrade is in progress	Wait until the upgrade has completed
10041	Cluster name not configured: if FindMe or clustering are in use a cluster name must be defined	Configure the cluster name
10042	Invalid clustering configuration: H.323 mode must be turned On - clustering uses H.323 communications between peers	Configure H.323 mode
10043	LDAP Configuration required: a valid Server Address, Server Port, BindDN and BaseDN are required if remote login authentication is used for administrator or FindMe users	Configure LDAP parameters
10044	TURN relays installed: TURN services are only available on VCS Expressway; TURN option key ignored	Add/Remove option keys
10045	TURN relay licenses required: TURN services are enabled but no TURN relay license option keys are installed	Add option key or disable TURN services
10046	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
10047	Restart required: QoS settings have been changed, however a restart is required for this to take effect	Restart the VCS
10048	Restart required: the TMS Agent service has stopped unexpectedly. If the problem persists, contact your Cisco support representative	Restart the VCS
10049	Reboot required: the advanced account security mode has changed, however a reboot is required for this to take effect	Reboot the VCS

ID	Warning message	Resolution
10050	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
10051	SNMP enabled: you are recommended to disable SNMP when in advanced account security mode	Configure SNMP mode
10052	NTP server problem: the VCS is unable to determine the correct time and date	Check the time configuration
10053	HTTPS client certificate validation: you are recommended to enable client side certificate validation for HTTPS connections when in advanced account security mode	Configure HTTPS client certificate validation
10054	HTTPS client certificate checking: client certificate checking mode has changed, however a restart is required for this to take effect	Restart the VCS
10055	Failed to load Call Policy file	Configure Call Policy
10056	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
10057	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
10058	Remote logging enabled: you are recommended to disable the remote syslog server when in advanced account security mode	Configure remote logging
10059	Incident reporting enabled: you are recommended to disable incident reporting when in advanced account security mode	Configure incident reporting
10060	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
10061	External manager has certificate checking disabled: you are recommended to enable external manager certificate checking when in advanced account security mode	Configure external manager
10062	Restart required: a language pack has been installed, however a restart is required for this to take effect	Restart the VCS
10063	Language pack mismatch: some text labels may not be translated	Contact your Cisco representative to obtain the correct language pack version
10064	VCS database failure	Contact your Cisco support representative
10073	Uncontrolled shutdown detected	Contact your Cisco representative if the problem persists

ID	Warning message	Resolution
10075	Restart required: cluster configuration has been changed, however a restart is required for this to take effect	Restart the VCS

Bibliography

Reference	Document number (if applicable)	Title	Link
1		ITU Specification: H.235 Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals	http://www.itu.int/rec/T-REC-H.235/en
2		ITU Specification: H.350 Directory services architecture for multimedia conferencing	http://www.itu.int/rec/T-REC-H.350/en
3		RFC 2782: A DNS RR for specifying the location of services (DNS SRV)	http://www.ietf.org/rfc/rfc2782.txt
4		RFC 3164: The BSD syslog Protocol	http://www.ietf.org/rfc/rfc3164.txt
5		RFC 3880: Call Processing Language (CPL): A Language for User Control of Internet Telephony Services	http://www.ietf.org/rfc/rfc3880.txt
6		DNS and BIND Fourth Edition, Albitz and Liu, O'Reilly and Associates, ISBN: 0-596-00158-4	
7		RFC 2915: The Naming Authority Pointer (NAPTR) DNS Resource Record	http://www.ietf.org/rfc/rfc2915.txt
8		RFC 3761: The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS)Application (ENUM)	http://www.ietf.org/rfc/rfc3761.txt
9		Mastering Regular Expressions, Jeffrey E.F. Friedl, O'Reilly and Associates, ISBN: 1-56592-257-3	
10		RFC 3327: Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts	http://www.ietf.org/rfc/rfc3327.txt
11		Session Traversal Utilities for NAT (STUN)	http://tools.ietf.org/html/rfc5389
12		Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)	http://tools.ietf.org/html/rfc5766
13		RFC 4787: Network Address Translation (NAT) Behavioral Requirements for Unicast UDP	http://www.ietf.org/rfc/rfc4787.txt
14		RFC 4028: Session Timers in the Session Initiation Protocol (SIP)	http://www.ietf.org/rfc/rfc4028.txt

Reference	Document number (if applicable)	Title	Link
15		ITU Specification: H.323: Packet-based multimedia communications systems	http://www.itu.int/rec/T-REC-H.323/en
16		RFC 3263: Session Initiation Protocol (SIP): Locating SIP Servers	http://www.ietf.org/rfc/rfc3263.txt
17		RFC 3550: RTP: A Transport Protocol for Real-Time Applications	http://www.ietf.org/rfc/rfc3550.txt
18		RFC 791: Internet Protocol	http://www.ietf.org/rfc/rfc791.txt
19		RFC 2460: Internet Protocol, Version 6 (IPv6) Specification	http://www.ietf.org/rfc/rfc2460.txt
20		RFC 3261: SIP: Session Initiation Protocol	http://www.ietf.org/rfc/rfc3261.txt
21		RFC 3489: STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)	http://www.ietf.org/rfc/rfc3489.txt
22		XML and Writing CPL for TANDBERG Infrastructure products Rev 1.2	www.tandberg.com
23		Management Information Base for Network Management of TCP/IP-based internets: MIB-II	http://www.ietf.org/rfc/rfc1213.txt
24	D14269	Cisco VCS Deployment Guide - Microsoft OCS 2007 (R1 and R2) and Cisco VCS Control	www.tandberg.com
25	D14366	Cisco VCS Multiway Deployment Guide	www.tandberg.com
26	D14368	Provisioning Deployment Guide	www.tandberg.com
27	D14367	Cisco VCS Deployment Guide - Cluster creation and maintenance	www.tandberg.com
28	D14350	Cisco VCS Getting Started Guide	www.tandberg.com
29	D14525	Cisco VCS Deployment Guide - FindMe	www.tandberg.com
30	D14526	Cisco VCS Deployment Guide - Authenticating Cisco VCS accounts using LDAP	www.tandberg.com
31	D14465	Cisco VCS Deployment Guide - ENUM dialing on Cisco VCS	www.tandberg.com
32	D14548	Cisco VCS Deployment Guide - Certificate creation and use with Cisco VCS	www.tandberg.com
33	D14524	Cisco VCS Deployment Guide - Basic Configuration - Single Cisco VCS Control	www.tandberg.com

Reference	Document number (if applicable)	Title	Link
34	D14618	Cisco VCS Deployment Guide - Cisco VCS Starter Pack Express	www.tandberg.com
35		RFC 3326: The Reason Header Field for the Session Initiation Protocol (SIP)	http://www.ietf.org/rfc/rfc3326.txt
36	D14602	Cisco VCS Deployment Guide - Cisco Unified Communications Manager with Cisco VCS using a SIP trunk	www.tandberg.com
37	D14652	Cisco VCS Deployment Guide - Microsoft OCS 2007, Cisco VCS Control and Cisco AM GW	www.tandberg.com
38		RFC 5245: Interactive Connectivity Establishment (ICE)	http://tools.ietf.org/html/rfc5245
39	D14049	Cisco TelePresence Video Communication Server Administrator Guide (this document)	www.tandberg.com
40	D14754	Cisco TelePresence Video Communication Server Command Reference	www.tandberg.com
41		RFC 5626: Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)	http://www.ietf.org/rfc/rfc5626.txt
42	D14651	Cisco VCS Deployment Guide - Basic Configuration - Cisco VCS Expressway with Cisco VCS Control	www.tandberg.com

Glossary

Term	Definition
A record	A type of DNS record that maps a host name to an IPv4 address.
AAAA record	A type of DNS record that maps a host name to an IPv6 address.
Administrator Policy	See Call Policy
Alias	The name an endpoint uses when registering with the Cisco VCS. Other endpoints can then use this name to call it. An endpoint may register with more than one alias.
Alternate	One or more Cisco VCSs configured to support the same zone in order to provide redundancy. See also Cluster.
AOR Address of Record	A SIP or SIPS URI that points to a domain with a location service that can map the URI to another URI where the user might be available. Typically, the location service is populated through registrations. An AOR is frequently thought of as the “public address” of the user.
ARQ Admission Request	An endpoint RAS request to make or answer a call.
Assent	Cisco’s proprietary protocol for firewall traversal.
Border Controller	A device used to control multimedia networks and firewall traversal.
CA Certificate authority	An organization that validates and signs certificate requests.
Call Policy	In relation to the Cisco VCS, the set of rules configured system-wide (either via the web interface or CPL script) that determine the action(s) to be applied to calls matching a given criteria. (Also referred to as Administrator Policy.)
Cisco TMS Cisco TelePresence Management Suite	A Cisco product used for the management of video networks.
Cisco VCS Cisco TelePresence Video Communication Server	A generic term for the Cisco product which acts as a gatekeeper and SIP proxy/server.
Cisco VCS Control	A Cisco VCS whose main function is to act as a gatekeeper, SIP proxy and firewall traversal client. This system is generally located within the firewall.
Cisco VCS Expressway	A Cisco VCS with the same functionality as a Cisco VCS Control that can also act as a firewall traversal server. This is generally located outside the firewall.
CLI Command line interface	A text-based user interface used to access the Cisco VCS.

Term	Definition
Cluster	A collection of between two and six Cisco VCSs that have been configured to work together as a single Local Zone, in order to provide scalability and redundancy.
Conference Factory	An application that allows the Cisco VCS to support the Multiway feature. See the Conference Factory section for more information.
CPL Call Processing Language	An XML-based language for defining call handling. Defined by *RFC 3880* [5].
CRL Certificate revocation list	A list from a CA (certificate authority) of previously signed certificates that it marks as no longer valid.
Default Subzone	A subzone used to represent locally registered endpoints and systems that do not fall within any other existing configured subzones within the Local Zone.
Default Zone	A pre-configured zone on the Cisco VCS used to represent incoming connections from endpoints that are not recognized as belonging to the Local Zone or any of the existing configured neighbor, traversal client or traversal server zones.
Device Provisioning	An option key that allows Cisco VCS to provision endpoints with configuration information on request and to supply endpoints with phone book information. See the Device Provisioning section for more information.
DiffServ Differentiated Services	A Quality of Service (QoS) mechanism supported by the Cisco VCS.
DNS Domain Name System	A distributed database linking domain names to IP addresses.
DNS zone	On the Cisco VCS, a zone used to configure access to endpoints located via a DNS lookup.
E.164	An ITU standard for structured telephone numbers. Each telephone number consists of a country code, area code and subscriber number.
ENUM E.164 Number Mapping	A means of mapping E.164 numbers to URIs using DNS. Defined by *RFC 3761* [8].
ENUM zone	On the Cisco VCS, a zone used to configure access to endpoints located via ENUM.
External manager	The remote system that is used to manage endpoints and network infrastructure. The Cisco TelePresence Management Suite (Cisco TMS) is an example of an external manager.

Term	Definition
External zone	Any zone configured on the local Cisco VCS that connects out to a remote system or the internet. Neighbor, traversal server, traversal client, ENUM and DNS zones are all external zones.
Firewall traversal	The act of crossing a firewall or NAT device.
FindMe™	Cisco TelePresence FindMe is a User Policy feature that allows users to have a single alias on which they can be reached regardless of the endpoints they are currently using.
FQDN Fully Qualified Domain Name	A domain name that specifies the node's position in the DNS tree absolutely, uniquely identifying the system or device. Note that in order to use FQDNs instead of IP addresses when configuring the Cisco VCS, you must have at least one DNS server configured.
Gatekeeper	A device used to control H.323 multimedia networks. An example is the TANDBERG Gatekeeper.
Gatekeeper zone	A collection of all the endpoints, gateways and MCUs managed by a single gatekeeper.
H.323	A standard that defines the protocols used for packet-based multimedia communications systems.
HTTP Hypertext Transfer Protocol	A protocol used for communications over the internet.
HTTPS Hypertext Transfer Protocol over Secure Socket Layer	A protocol used for secure communications over the internet, combining HTTP with TLS.
Hop count	The maximum number of gatekeeper or SIP proxy devices (e.g. a Cisco VCS) that a message may be forwarded through before it is decided that its intended recipient is not reachable.
ICE Interactive Connectivity Establishment	A collaborative algorithm that works together with STUN services (and other NAT traversal techniques) to allow clients to achieve firewall traversal. This is the emerging traversal standard for use by SIP endpoints (although it could be used for other protocols).
IETF Internet Engineering Task Force	An organization that defines (via documents such as RFCs) the protocol standards and best practices relating to the design, use and management of the internet.
Interworking	Allowing H.323 systems to connect to SIP systems.
IPsec Internet Protocol Security	A protocol suite for securing IP communications. It is used by the Cisco VCS to establish secure communication between cluster peers.
IPv4 Internet Protocol version 4	Version 4 of the Internet Protocol, defined in *RFC 791* [18].

Term	Definition
IPv6 Internet Protocol version 6	Version 6 of the Internet Protocol, defined in *RFC 2460* [19].
IRQ Information Request	A request sent to an endpoint requesting information about its status.
LAN Local Area Network	A geographically limited computer network, usually with a high bandwidth throughput.
LDAP Lightweight Directory Access Protocol	A protocol for accessing on-line directories running over TCP/IP.
Link	In relation to the Cisco VCS, a connection between two nodes.
Local call	(Also referred to as a non-traversal call.) A call where the signaling but not the media is routed through the local Cisco VCS. See the What are traversal calls? section for more information.
Local registration, Locally registered endpoint	A relative term used to refer to any endpoint or system that is registered with the local Cisco VCS.
Local Cisco VCS	A relative term used to refer to the particular Cisco VCS that you are currently administering, as opposed to other Cisco VCSs in your network.
Local Zone	A relative term used to refer to the group of endpoints and other systems registered to a particular Cisco VCS. If a Cisco VCS is part of a cluster, the Local Zone refers to the collection of all endpoints and other systems registered to all peers in that cluster.
LRQ Location Request	A RAS query between gatekeepers to determine the location of an endpoint.
MCU Multipoint Control Unit	A network device that allows multiple endpoints to participate in a video conference.
Microsoft Office Communications Server 2007 Microsoft OCS	Microsoft OCS (Office Communications Server) 2007 is an enterprise real-time communications server, providing the infrastructure to allow instant messaging, presence, audio-video conferencing and web conferencing functionality.
Microsoft Office Communications (MOC) client	The client application released with Microsoft Office Communications Server (OCS). The MOC client can be used for instant messaging, presence, voice and video calls and ad hoc conferences.
Multiway	Cisco TelePresence Multiway enables endpoint users to create a conference while in a call even if their endpoint does not have this functionality built in. See the Conference Factory section for more information.
NAPTR record	A type of DNS record.

Term	Definition
NAT Network Address Translation	Also known as IP masquerading. Rewriting source and destination addresses as the IP packet passes through the NAT device.
Neighbor	A remote system to which the Cisco VCS has a connection via a neighbor zone.
Neighbor zone	On the Cisco VCS, a zone used to configure a connection to a remote system with which the local Cisco VCS has a non-traversal relationship.
Node	In relation to the Cisco VCS, a node is one end of a link. A node can be a local subzone or a zone.
Non-traversal call	(Also referred to as a local call.) A call where the signaling but not the media is routed through the local Cisco VCS. See the What are traversal calls? section for more information.
NTP Network Time Protocol	A protocol used for synchronizing clocks. Defined in *RFC 1305*.
OCS Relay	A Cisco VCS application that enables interoperability between Microsoft Office Communications Server (OCS) and FindMe. See the OCS Relay section for more information.
Peer	A Cisco VCS that has been configured to belong to a cluster.
PEM Privacy-Enhanced Electronic Mail	An IETF proposal for securing messages using public key cryptography.
Pipe	In relation to the Cisco VCS, a means of controlling the bandwidth used on a link.
Proxy, Proxy server	In SIP, an intermediary entity that acts as both a server and a client for the purpose of making requests on behalf of other clients. A proxy server primarily plays the role of routing, which means its job is to ensure that a request is sent to another entity “closer” to the targeted user. Proxies are also useful for enforcing policy (for example, making sure a user is allowed to make a call). A proxy interprets, and, if necessary, rewrites specific parts of a request message before forwarding it. While a proxy can set up calls between SIP endpoints, it does not participate in the call after it is set up.
QoS Quality of Service	Mechanisms that give a network administrator the ability to provide different priorities to an applications' network traffic.
RAS Registration, Admission and Status	A protocol used between H.323 endpoints and a gatekeeper to register and place calls.
Registrar	In SIP, a server that accepts REGISTER requests and places the information it receives in those requests into the location service for the domain it handles. This information is used to advise other SIP Proxies/Registrars where to send calls for that endpoint.

Term	Definition
Regex Regular expression	A pattern used to match text strings according to a POSIX-defined syntax.
RFC Request for Comments	A process and result used by the IETF for Internet standards.
RS-232	A commonly used standard for computer serial ports.
RTCP RTP Control Protocol	A control protocol for RTP. Defined by *RFC 3550* [17].
RTP Real-time Transport Protocol	Real time protocol designed for the transmission of voice and video. Defined by *RFC 3550* [17].
SASL Simple Authentication and Security Layer	A framework for authentication and data security in Internet protocols.
SSH Secure Shell	An encrypted protocol used to provide a secure CLI.
SIMPLE Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions	An instant messaging and presence protocol based on SIP.
SIP Session Initiation Protocol	IETF protocol for controlling multimedia communication. Defined by *RFC 3261* [20].
SNMP Simple Network Management Protocol	A protocol used to monitor network devices.
Source alias	The alias present in the “source” field of a message.
SRV record Service record	A type of DNS record. Defined by *RFC 2782* [3].
STUN Simple Traversal of UDP through NAT	Firewall NAT traversal for SIP. Defined by *RFC 3489* [21].
Subzone	A segment within a Cisco VCS Local Zone used to control the bandwidth used by various parts of your network, and to control registrations.
TCP Transmission Control Protocol	A reliable communication protocol defined by *RFC 791* [18].

Term	Definition
Telnet	A network protocol used on the internet or Local Area Networks (LANs).
TLS Transport Layer Security	A protocol that provides secure communications over the internet.
TMS	See Cisco TMS.
TMS Agent	An internal Cisco VCS feature used to manage FindMe and Device Provisioning data. See the TMS Agent section for more information.
Transform	In relation to the Cisco VCS, the process of changing or replacing the alias being searched for.
Traversal call	Any call where both signaling and media are routed through the local Cisco VCS. See the What are traversal calls? section for more information.
Traversal client	A traversal entity on the private side of a firewall. Examples are a Cisco VCS Control or Gatekeeper.
Traversal client zone	A zone on a Cisco VCS traversal client that has been used to configure a connection to a particular traversal server.
Traversal server	A traversal entity on the public side of a firewall. Examples are the Cisco VCS Expressway or Border Controller.
Traversal server zone	A zone on a Cisco VCS Expressway that has been used to configure a connection to a particular traversal client.
Traversal Subzone	A conceptual subzone through which all traversal calls are deemed to pass; used to manage the bandwidth of traversal calls.
Traversal-enabled endpoint	Any endpoint that supports the Assent and/or ITU H.460.18 and H.460.19 standards for firewall traversal. This includes all Cisco TelePresence MXP endpoints.
TURN Traversal Using Relays around NAT	Relay extensions to STUN (Session Traversal Utilities for NAT).
UA User Agent	A SIP device used to make and receive calls.
UDP User Datagram Protocol	A communication protocol defined by *RFC 791* [18]. It is less reliable than TCP.
URI Uniform Resource Identifier	A formatted string used to identify a resource, typically on the internet.
User Policy	The set of rules that determines the actions to be applied to calls for a particular user or group. The Cisco VCS uses FindMe for its User Policy.
VCS	See Cisco VCS.
VCS Control	See Cisco VCS Control.

Term	Definition
VCS Expressway	See Cisco VCS Expressway.
Zone	Zones are used on the Cisco VCS to define and configure connections to locally registered and external systems and endpoints. The Local Zone refers to all the locally registered endpoints and systems, and consists of configurable subzones. External zones are used to configure connections to external systems with which the Cisco VCS has a neighbor, traversal client or traversal server relationship, and to configure the way in which the Cisco VCS performs ENUM and DNS searches.

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 © 2010, Tandberg Telecom UK Limited. All rights reserved.

TANDBERG is now part of Cisco. Tandberg Telecom UK Limited is a wholly owned subsidiary of Cisco Systems, Inc.

This product includes copyrighted software licensed from others. A list of the copyright notices and the terms and conditions of use can be found at: http://www.tandberg.com/collateral/documentation/User_Manuals/Cisco_VCS_EULA.pdf and http://www.tandberg.com/collateral/documentation/User_Manuals/Cisco_VCS_Copyrights.pdf.

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.

Patent information

This product is covered by one or more of the following patents:

- US7,512,708
- EP1305927
- EP1338127

A complete list of patents is available at: http://www.tandberg.com/tandberg_pm.jsp.

Disclaimers and notices

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.