Cisco Expressway
Configuration Report

Sample Report Expressway

As-Built Documentation for project

October 21, 2019

Document Information - Universal

Version Status

Release Number	Date	Reason for Version
1.0	October 21, 2019	Release

Client Information

Prepared for:	Large Company Inc.
Name:	H. Boss
Title:	CEO
Address:	Corporate Way
Telephone:	1 (555) 56987424
Email:	hboss@largecompany.com

Presenter Information

Prepared by:	Config Reports Ltd.
Name:	Jennifer SMITH
Title:	Ms.
Address:	22 Main Street
Telephone:	123456787
Email:	JSmith@email.com

Table of Content

1 Report Information

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

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

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

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

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

Optional packages that you can deploy include FindMe, Device Provisioning, and Advanced Networking (VCS Expressway only).

1.1 Report Summary

This report was generated with the following settings.

Report Info	
Report Date	21/10/2019 4:06:29 PM
Report generated for	Sample Report Expressway
Description	As-Built Documentation for project
Server Info	
Expressway version	X12.5.5
Expressway IP	10.5.1.130
Report Settings	
Report Type	Direct Report
Visual Style	Blu Dark.css
Report Content	All objects
Template HTML	Expressway_ReportTemplate.htm
Template Word	Triangle_Blue-universal.doc
Report Tool Info	
Report Tool Version	12.0.19 / 19 Oct 2019
Report Tool License	Licensed [Prof all]

2 Information

The following section provides details of the software, hardware, and time settings of the Expressway.

System Information	
General	
System name	ExpWay1255
Product	TANDBERG VCS
Software	
Software version	X12.5.5
Software build	oak_v12.5.5_rc_1
Software release date	2019-08-14
Software name	s42700
Software Release Key	

Hardware	
Hardware version	VMware
Serial number	0C95079E
Time Information	
System time (UTC)	2019-10-21 14:06:26
Time zone	Etc/GMT+1
Local time	2019-10-21 14:06:26
Uptime	6 days 23 hours 53 minutes 55 seconds
Options	
Non-Traversal Calls	1
Traversal Calls	1
Registrations	3
TPRoom	0
TURN Relays	
Expressway	False
Encryption	True
Interworking	False
FindMe	True
Dual Network Interfaces	False
Advanced Account Security	False
Starter Pack	False
Enhanced OCS Collaboration	False
ExpresswaySeries	False

3 System

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

3.1 Administration

The System Administration shows the name of the Cisco TelePresence Video Communication Server system and methods by which the system may be accessed by administrators. Although you can administer the Cisco TelePresence Video Communication Server through a PC connected directly to the unit with a serial cable, you may want to access the system remotely over IP. You can do this using the web interface via HTTPS, or through a command line interface via SSH. Configurable options are for:

- System Name
- Ephemeral Port Range
- Services
- Session Limits
- System Protection
- Web Server Configuration

Administration	
System Name	
System name	ExpWay1255
Ephemeral Port Range	
Start	31111
End	35999
Services	
Serial port / console	On
SSH service	On
Web interface (over HTTPS)	On
Session Limits	

Session time out (minutes)	90
Per-account session limit	150
System session limit	55
System Protection	
Automatic discovery protection	On
Web Server Configuration	
Redirect HTTP requests to HTTPS	On
HTTP strict transport security (HSTS)	On
Client certificate-based security	NotRequired

3.2 Network Interfaces

This section shows settings for:

- Ethernet
- IP
- Static Routes

3.2.1 Ethernet

This section shows configuration of speed for the connections between the Expressway and the Ethernet networks to which it is connected. The speed and duplex mode must be the same at both ends of the connection. If you installed the Advanced Networking option, you can configure the speed and duplex mode for each Ethernet port. The default Speed is Auto, which means that the Expressway and the connected switch will automatically negotiate the speed and duplex mode.

Ethernet	
Name	**Details**
LAN 1	MAC address: 00:0C:29:79:43:3A Speed: 10000full IP Address: 10.5.1.130 IP Mask: 255.255.255.0

3.2.2 IP

The IP section shows configuration of the IP protocols and network interface settings of the Expressway. Expressway can be configured to use IPv4, IPv6 or Both protocols. The default is Both.

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

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

Ethernet	
Name	**Details**
Configuration	IP protocol: IPv4 Use dual network interfaces: No External LAN interface: IPv4 gateway: 10.5.1.1
LAN 1 - Internal	IPv4 Address: 10.5.1.130 IPv4 subnet Mask: 255.255.255.0 IPv4 static NAT mode: IPv4 static NAT address:

3.2.3 Static Routes

This section shows Static Routes from the Expressway to an IPv4 or IPv6 address range.

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

Static Routes		
Name	**Details**	
10.5.1.0	IP address	10.5.1.0
	Prefix length	24
	Gateway	10.5.1.131
	Interface	Auto
77.77.0.0	IP address	77.77.0.0
	Prefix length	16
	Gateway	10.5.1.1
	Interface	Auto
99.99.99.99	IP address	99.99.99.99
	Prefix length	32
	Gateway	10.5.1.1
	Interface	Auto

3.3 DNS

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

DNS			
DNS Settings			
System host name	EW1255		
Domain name	lab.test		
DNS requests port range	Use the ephemeral port range		
Default DNS servers			
Address 1	10.5.1.166		
Address 2	8.8.8.8		
Address 3	8.8.4.4		
Address 4			
Address 5			
Per-domain DNS Servers			
Per-domain DNS servers	**Server**	**Address**	**Domain names**
	Server 1	10.5.1.166	lab.test

3.4 Time

The Time section shows configuration of the Expressway's NTP servers and the local time zone. An NTP server is a remote server with which the Expressway synchronizes in order to ensure its time is accurate. The NTP server provides the Expressway with UTC time. Accurate time is necessary for correct system operation.

Time		
Name	**Details**	
NTP Servers		
NTP servers	**Server name**	**Address**
	NTP Server 1	0.ntp.tandberg.com
	NTP Server 2	1.ntp.tandberg.com

Time		
Name	**Details**	
	NTP Server 3	2.ntp.tandberg.com
	NTP Server 4	10.5.1.100
Time Zone		
Time zone	Etc/GMT+1	

3.5 SNMP

This section shows the Expressway's SNMP settings. Tools such as Cisco TelePresence Management Suite (Cisco TMS) or HP OpenView may act as SNMP Network Management Systems (NMS). They allow monitoring of network devices, including the Expressway, for conditions that might require administrative attention. The Expressway supports the most basic MIB-II tree (.1.3.6.1.2.1) as defined in RFC 1213. The information made available by the Expressway includes the following:

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

By default, SNMP is Disabled, therefore to allow the Expressway to be monitored by an SNMP NMS (including Cisco TMS), alternative SNMP mode must be selected.

SNMP	
Configuration	
SNMP mode	v3 plus TMS support
Description	SNMPv2
Community name	public
System contact	Administrator
Location	OurSNMPLocation
Username	admin
v3 Authentication	
Authentication mode	off

3.6 Clustering

An Expressway can be part of a cluster of up to six Expressways. Each Expressway in the cluster is a peer of every other Expressway in the cluster. When creating a cluster, the cluster name should be defined and one peer must be nominated as the master from which all relevant configurations are replicated to the other peers in the cluster. Clusters are used to:

- Increase the capacity of your Expressway deployment compared with a single Expressway.
- Provide redundancy in the rare case that an Expressway becomes inaccessible (for example, due to a network or power outage) or while it is in maintenance mode (for example, during a software upgrade).

Clustering	
Configuration	
Cluster name (FQDN for provisioning)	excluster.lab.test
Configuration master	1
Peer 1 IP address	1.2.3.4
Peer 2 IP address	
Peer 3 IP address	
Peer 4 IP address	
Peer 5 IP address	
Peer 6 IP address	
Cluster Address Mapping	

Cluster address mapping enabled	False

3.7 Protection

The Protection section shows settings for intruder protection, used to detect and block malicious traffic and to help protect the VCS from dictionary-based attempts to breach login security.

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

The report shows the Automated Detection Configuration, Exemptions and Blocked Addresses.

3.7.1 Automated Detection

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

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

3.7.1.1 Configuration

The Configuration is used to enable and configure the VCS's protection categories, and to view current activity.

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

Automated detection overview										
Name	Description	Enabled	Detection window (sec.)	Trigger level	Block duration (sec.)	Total blocked	Currently blocked	Total failures	Currently failures	Excluded addresses
web-intrusion		True	600	5	600	0	0	0	0	
apache-auth		True	600	5	600	0	0	1	0	
sshpfwd-intrusion		True	600	5	600					
ssh-intrusion		True	600	5	600	0	0	0	0	
ssh-auth		True	600	5	600	0	0	0	0	
sip-violations		False	600	5	600					
http-ce-intrusion		True	600	5	600					
web-auth		True	600	5	600	0	0	2	0	
sip-reg		False	600	5	600					
sip-auth		False	600	5	600					
xmpp-intrusion		True	600	5	600					
http-ce-auth		True	600	5	600					
sshpfwd-auth		True	600	5	600					
http-ce-resource_access		False	600	5	600					

3.7.1.2 Exemptions

The Exemptions section shows IP addresses that are to be exempted always from one or more protection categories.

< No records found >

3.8 Quality of Service

The Quality of Service (QoS) shows configuration of QoS options for outbound traffic from the Expressway. This allows the network administrator to tag all signalling and media packets flowing through the Expressway with one specific QoS tag and hence provide the ability to prioritize video traffic over normal data traffic. Management traffic, for example SNMP messages, is not tagged.

Quality of Service	
Configuration	
DSCP Signaling value	21
DSCP Audio value	22
DSCP Video value	23
DSCP XMPP value	24

3.9 External Manager

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

External Manager	
Configuration	
Address	10.5.1.1
Path	tms/public/external/management/SystemManagementService.asmx
Protocol	HTTP
Certificate verification mode	Off

4 Configuration

This section shows settings for:

- Protocols
- Registration
- Authentication
- Call Routing
- Local Zone
- Zones
- Dial Plan
- Bandwidth
- Traversal
- Call Policy
- Unified Communications

4.1 Protocols

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

- Configuring H.323
- Configuring SIP
- Configuring domains
- Configuring SIP and H.323 interworking

4.1.1 H.323

The H.323 shows configuration for H.323 settings on the Expressway, including whether H.323 is enabled or not, Gatekeeper and Gateway settings.

H.323	
Configuration	
H.323 mode	On

Gatekeeper	
Registration UDP port	1719
Registration conflict mode	Overwrite
Call signaling TCP port	1720
Call signaling port range start	15000
Call signaling port range end	19999
Time to live	1800
Call time to live	120
Auto discover	On
Gateway	
Caller ID	IncludePrefix

4.1.2 SIP

The SIP section shows the configuration for SIP settings on the Expressway, including:

- SIP functionality and SIP-specific transport modes and ports
- Certificate revocation checking modes for TLS connections
- Registration Controls
- Authentication
- Advanced settings with SIP Maximum Size and the TCP Connect Timeout.

SIP	
Configuration	
SIP mode	Off
UDP mode	Off
UDP port	5060
TCP mode	Off
TCP port	5060
TLS mode	On
TLS port	5061
Mutual TLS mode	Off
Mutual TLS port	5062
TCP outbound port start	25000
TCP outbound port end	29999
Session refresh interval (seconds)	1800
Minimum session refresh interval (seconds)	500
TLS handshake timeout (seconds)	5
Certificate Revocation Checking	
Certificate revocation checking mode	Off
Registration Controls	
Standard registration refresh strategy	Maximum
Standard registration refresh minimum (seconds)	45
Standard registration refresh maximum (seconds)	60
Outbound registration refresh strategy	Variable
Outbound registration refresh minimum (seconds)	300
Outbound registration refresh maximum (seconds)	3600
SIP registration proxy mode	Off
Advanced	
SIP max size	32768
SIP TCP connect timeout	10
SIP Tls DH key size	1024
SIP Tls versions	TLSv1.2

4.1.3 Interworking

The Interworking section contains configurations indicating whether or not the Expressway acts as a gateway between SIP and H.323 calls. The translation of calls from one protocol to the other is known as "interworking".

Interworking	
Configuration	
H.323 <-> SIP interworking mode	Registered Only

4.2 Registration

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

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

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

4.2.1 Registration Configuration

The Registration configuration page is used to control how the VCS manages its registrations, with the Registration Policy setting to be used while determining which endpoints may register with the system.

- **None:** no restriction.
- **Allow List:** only endpoints attempting to register with an alias listed on the Allow List may register.
- **Deny List:** all endpoints, except those attempting to register with an alias listed on the Deny List, may register.
- **Policy service:** only endpoints that register with details allowed by the remote policy service may register. This option comes with its own settings
- Default: None

Registration Configuration	
Configuration	
Restriction Policy	PolicyService
Protocol	HTTPS
Certificate verification mode	On
HTTPS certificate revocation list (CRL) checking	Off
Server 1 address	10.5.1.166
Server 2 address	
Server 3 address	
Path	
Status path	status
Username	
Default CPL	<reject status='504' reason='Registration Policy Unavailable'/>

4.2.2 Registration Allow List

The Registration Allow List shows the endpoint aliases and alias patterns that are allowed to register with the VCS. Only one of an endpoint's aliases needs to match an entry in the Allow List for the registration to be allowed. A Restriction policy must be selected to use the Allow List.

Registration Allow List		
Pattern String	**Pattern Type**	**Description**
(23432...)	Regex	Allow Patt one

Registration Allow List		
Pattern String	**Pattern Type**	**Description**
55.55.5.5	Exact	Allow Patt Two

4.2.3 Registration Deny List

The Registration Deny List section shows the endpoint aliases and alias patterns that are not allowed to register with the VCS. Only one of an endpoint's aliases needs to match an entry in the Deny List for the registration to be denied. A Restriction policy must be selected to use the Deny List.

Registration Deny List		
Pattern String	**Pattern Type**	**Description**
5556666	Suffix	Deny Patt. One
(32423423...)	Regex	Deny Patt. Two

4.3 Authentication

This section provides information about the VCS's authentication policy with the Outbound Connection Credentials and Devices.

4.3.1 Outbound Connection Credentials

The Outbound Connection Credentials section shows the username that VCS will use whenever it is required to authenticate with external systems.

Outbound Connection Credentials	
Configuration	
Authentication username	test

4.3.2 Devices

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

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

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

4.3.2.1 Local Database

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

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

Same credentials can be used by more than one device.

Local Database
Name
test
test3
test2

4.3.2.2 Active Directory Service

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

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

If Active Directory (direct) authentication has been configured and NTLM protocol challenges is set to Auto, then NTLM authentication challenges are offered to those devices that support NTLM. Devices that do not support NTLM will continue to receive a standard Digest challenge.

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

Active Directory Service	
Configuration	
Connect to active directory service	On
NTLM protocol challenges	Auto

4.3.2.3 H.350 Directory Service

This section shows the Device authentication H.350 configuration for connection via LDAP to an H.350 directory service. An H.350 directory service lookup can be used for authenticating any endpoint, SIP and H.323.

H.350 Directory Service	
H.350 Directory Service Configuration	
H.350 device authentication	Off
Source of aliases for registration	H.350 directory
LDAP Server Configuration	
Server address	10.5.1.1
FQDN address resolution	AddressRecord
Port	636
Encryption	TLS
Authentication Configuration	
Bind DN	test
Directory Configuration	
Base DN for devices	test

4.4 Call Routing

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

- Locally registered endpoints
- Neighboring systems, including neighbors, traversal clients and traversal servers
- Endpoints on the public internet

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

It is important to understand the process before setting up dial plan so that circular references can be avoided, where an alias is transformed from its original format to a different format, and then back to the original alias. The VCS is able to detect circular references. If it identifies one it will terminate that branch of the search and return a "policy loop detected" error message.

Call Routing	
Configuration	
Call signaling optimization	Off

Call loop detection mode	On

4.5 Local Zone

This section shows collection of all endpoints, gateways, MCUs and Content Servers registered with the VCS makes up its Local Zone. The Local Zone is divided into subzones. These include an automatically created Default Subzone and up to 1000 manually configurable subzones. When an endpoint registers with the VCS it 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 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 the VCS is part of a cluster

4.5.1 Default Subzone

This section shows Default Subzones used to place bandwidth restrictions on calls involving endpoints in the Default Subzone, and to specify the Default Subzone's registration, authentication and media encryption policies.

When an endpoint registers with the VCS, its IP address and alias is checked against the subzone membership rules and it is assigned to the appropriate subzone. If no subzones have been created, or the endpoint's IP address or alias does not match any of the subzone membership rules, it is assigned to the Default Subzone (subject to the Default Subzone's Registration policy and Authentication policy).

The use of a Default Subzone on its own (without any other manually created subzones) is suitable only if uniform bandwidth available between all endpoints. Note that if a Local Zone contains two or more different networks with different bandwidth limitations, separate subzones for each different part of the network should be configured.

Default Subzone	
Policy	
Registration policy	Allow
Authentication policy	Do not check credentials
SIP	
Media encryption mode	Auto
ICE supports	Off
Multistream mode	On
AES GCM support	Off
SIP UPDATE for session refresh	On
Total Bandwidth Available	
Bandwidth restriction	NoBandwidth
Bandwidth limit (kbps)	500000
Calls Into or Out of the Default Subzone	
Bandwidth restriction	Unlimited
Per call bandwidth limit (kbps)	na
Calls Entirely Within This Subzone	
Bandwidth restriction	Limited
Per call bandwidth limit (kbps)	1920

4.5.2 Traversal Subzones

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 allows 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.

Traversal Subzone	
Ports	
Traversal media port start	36000
Traversal media port end	59999

Total Bandwidth Available	
Bandwidth restriction	Unlimited
Bandwidth limit (kbps)	na
Calls Handled by Traversal Subzone	
Bandwidth restriction	Unlimited
Per call bandwidth limit (kbps)	na

4.5.3 Subzones

The Local Zone's subzones are used for bandwidth management and to control registration and authentication policies.

The Subzones lists all the subzones that have been configured on the VCS, and allows one 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, the Subzone membership rules should be set up to control which subzone an endpoint device is assigned to when it registers with the VCS as opposed to defaulting to the Default Subzone.

Subzones	
Name	**Details**
subzone1	**Policy**
	Registration policy: Allow
	Authentication policy: Treat as authenticated
	SIP
	Media encryption mode: Auto
	ICE supports: Off
	Multistream mode: On
	AES GCM support: Off
	SIP UPDATE for session refresh: Off
	Total Bandwidth Available
	Bandwidth restriction: Unlimited
	Bandwidth limit (kbps): na
	Calls Into or Out Of This Subzone
	Bandwidth restriction: Limited
	Per call bandwidth limit (kbps): 1920
	Calls Entirely Within This Subzone
	Bandwidth restriction: NoBandwidth
	Per call bandwidth limit (kbps): 1920
subzone2	**Policy**
	Registration policy: Deny
	Authentication policy: Treat as authenticated
	SIP
	Media encryption mode: Auto
	ICE supports: Off
	Multistream mode: On
	AES GCM support: Off
	SIP UPDATE for session refresh: Off
	Total Bandwidth Available
	Bandwidth restriction: Unlimited
	Bandwidth limit (kbps): na
	Calls Into or Out Of This Subzone
	Bandwidth restriction: Unlimited
	Per call bandwidth limit (kbps): na
	Calls Entirely Within This Subzone
	Bandwidth restriction: Unlimited

Subzones	
Name	**Details**
	Per call bandwidth limit (kbps): na

4.5.4 Subzone Membership Rules

The Subzone membership rules section shows configuration of the rules that determine, based on the address of the device, to which subzone an endpoint is assigned when it registers with the VCS.

The page lists all the subzone membership rules that have been configured on the VCS, and lets one to create, edit, delete, enable and disable rules. Rule properties include:

- rule name and description
- priority
- the subnet or alias pattern matching configuration
- the subzone to which endpoints whose addresses satisfy this rule are assigned

Note that if an endpoint's IP address or registration alias does not match any of the membership rules, it is assigned to the Default Subzone. Up to 3000 subzone membership rules can be configured.

Subzone Membership Rules		
Name	**Details**	
Subzone Membership rule 1	**Configuration**	
	Rule name	Subzone Membership rule 1
	Description	Our SMR
	Priority	100
	Type	Subnet
	Subnet address	10.5.1.13
	Prefix length	32
	Target subzone	subzone1
	State	Enabled

4.6 Zones

The Zone status lists all of the external zones on the VCS. It shows the number of calls and amount of bandwidth being used by each zone.

The list of zones always includes the Default Zone, plus any other zones that have been created.

4.6.1 Zones

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

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

Zones			
Name	**Type**	**Details**	
Default zone	DefaultZone	**Policy**	
		Authentication policy	Do not check credentials
		SIP	
		Media encryption mode	Auto
		ICE support	Off
		Multistream mode	On
		Enable Mutual TLS on Default Zone	Off

Zones

Name	Type	Details
Zone1234567	Neighbor	**Configuration** Name: Zone1234567 Hop count: 15 **H323** Mode: On Port: 1719 **SIP** Mode: On Port: 50619 Transport: TLS TLS verify mode: Off Accept proxied registrations: Allow Media encryption mode: Auto ICE support: Off Preloaded SIP routes support: On AES GCM support: On SIP UPDATE for session refresh: On **Authentication** Authentication policy: Do not check credentials SIP authentication trust mode: Off **Location** Peer 1 address: 99.99.99.2 Peer 2 address: 10.5.1.2 Peer 3 address: Peer 4 address: Peer 5 address: Peer 6 address: **Advanced** Zone profile: CiscoUnifiedCommunicationsManagerPost9
zone2	ENUM	**Configuration** Name: zone2 Hop count: 15 **DNS Settings** DNS suffix: lab.test **H.323** Mode: On **SIP** Mode: On
CEtcp-10.5.1.120	Neighbor	**Configuration** Name: CEtcp-10.5.1.120 Hop count: 70 **H323** Mode: Off **SIP** Mode: On Port: 5060

Zones

Name	Type	Details
		Transport: TCP Accept proxied registrations: Allow Media encryption mode: CucmBestEffort ICE support: Off Preloaded SIP routes support: Off AES GCM support: Off SIP UPDATE for session refresh: On **Authentication** Authentication policy: Treat as authenticated SIP authentication trust mode: Off **Location** Peer 1 address: 10.5.1.120 Peer 2 address: Peer 3 address: Peer 4 address: Peer 5 address: Peer 6 address: **Advanced** Zone profile: Unified Communications
CEtcp-10.5.1.150	Neighbor	**Configuration** Name: CEtcp-10.5.1.150 Hop count: 70 **H323** Mode: Off **SIP** Mode: On Port: 5060 Transport: TCP Accept proxied registrations: Allow Media encryption mode: CucmBestEffort ICE support: Off Preloaded SIP routes support: Off AES GCM support: Off SIP UPDATE for session refresh: Off **Authentication** Authentication policy: Treat as authenticated SIP authentication trust mode: Off **Location** Peer 1 address: 10.5.1.150 Peer 2 address: Peer 3 address: Peer 4 address: Peer 5 address: Peer 6 address: **Advanced** Zone profile: Unified Communications
ZoneDNSyo	DNS	**Configuration** Name: ZoneDNSyo Hop count: 15

Zones

Name	Type	Details
		H.323
		Mode: On
		SIP
		Mode: On
		TLS verify mode: Off
		Fallback transport protocol: UDP
		Media encryption mode: Auto
		ICE support: Off
		AES GCM support: On
		SIP UPDATE for session refresh: On
		Preloaded SIP routes support: Off
		Authentication
		SIP authentication trust mode: Off
		Advanced
		Include address record: Off
		Zone profile: Default
ZONEtravclient	TraversalClient	**Configuration**
		Name: ZONEtravclient
		Hop count: 15
		Connection Credentials
		Username: admin
		H323
		Mode: On
		Protocol: Assent
		Port: 15246
		SIP
		Mode: On
		Port: 15247
		Transport: TLS
		TLS verify mode: Off
		Accept proxied registrations: Allow
		Media encryption mode: Auto
		ICE support: Off
		SIP poison mode: Off
		Preloaded SIP routes support: Off
		SIP parameter preservation: Off
		AES GCM support: On
		SIP UPDATE for session refresh: On
		Authentication
		Authentication policy: Do not check credentials
		Accept delegated credential checks: Off
		Client Settings
		Retry interval: 120
		Location
		Peer 1 address: 10.5.1.120
		Peer 2 address:
		Peer 3 address:
		Peer 4 address:
		Peer 5 address:

Zones		
Name	**Type**	**Details**
		Peer 6 address:
UCTraversalZone	EdgeTC	**Configuration** Name: UCTraversalZone Hop count: 15 **Connection Credentials** Username: admin **SIP** Port: 12385 Accept proxied registrations: Allow ICE support: Off SIP poison mode: Off Preloaded SIP routes support: Off SIP parameter preservation: Off **Authentication** Authentication policy: DoNotCheckCredentials Accept delegated credential checks: Off **Client Settings** Retry interval: 120 **Location** Peer 1 address: 10.5.1.166 Peer 2 address: Peer 3 address: Peer 4 address: Peer 5 address: Peer 6 address:

4.7 Domains

The Domains lists the SIP domains managed by this VCS.

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

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

Up to 200 domains can be configured.

Domains	
Name	**Details**
lab1.test	Index: 1 Domain name: lab1.test SIP registrations and provisioning on VCS: True SIP registrations and provisioning on Unified CM: False IM and Presence Service: False XMPP federation: False Deployment: 1
lab2.test	Index: 2 Domain name: lab2.test SIP registrations and provisioning on VCS: True SIP registrations and provisioning on Unified CM: False

Domains		
Name	**Details**	
	IM and Presence Service	False
	XMPP federation	False
	Deployment	1
lab3.test	Index	3
	Domain name	lab3.test
	SIP registrations and provisioning on VCS	True
	SIP registrations and provisioning on Unified CM	False
	IM and Presence Service	False
	XMPP federation	False
	Deployment	1

4.8 Unified Communications

This section shows configuration for the VCS Control and VCS Expressway for Unified Communications functionality, a core part of the Cisco Collaboration Edge Architecture. The section show settings for:

- Configuration
- Deployments
- Unified CM servers
- IM and Presence Service Nodes
- Unity Connection Servers
- Jabber Guests

4.8.1 Configuration

This section shows the settings for Unified Communications mode and related attributes.

Unified Communications	
Configuration	
Unified Communications mode	Mobile and remote access
MRA Access Control	
Authentication path	SAML SSO authentication
Authorize by OAuth token with refresh	False
Authorize by user credential	False
Allow Jabber iOS clients to use embedded Safari browser	False
Check for internal authentication availability	False
Allow activation code onboarding	False
Authorize by OAuth token	False
Advanced	
Maximum authorizations per period	8
Rate control period (seconds)	311

4.8.2 Deployments

A deployment is an abstract boundary used to enclose a domain and one or more Unified Communications service providers, such as Unified CM, Cisco Unity Connection, and IM and Presence Service nodes.

The purpose of multiple deployments is to partition the Unified Communications services available to mobile and remote access (MRA) users. This enables different subsets of MRA users to access different sets of services over the same VCS pair.

Deployments
Deployment Name
Default deployment
Deployment1
Deployment2

4.8.3 Unified CM Servers

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

Unified Communications	
Publisher Address	**Nodes discovered by this lookup**
10.5.1.120	
10.5.1.150	

4.8.4 IM and Presence Service Nodes

This section lists any IM and Presence Service nodes that have already been discovered.

IM and Presence Service Nodes	
Publisher Address	**Nodes discovered by this lookup**
10.5.1.122	10.5.1.122

4.8.5 Unity Connection Servers

This section lists any Cisco Unity Connection nodes that have already been discovered.

Unity Connection Servers	
Publisher Address	**Nodes discovered by this lookup**
10.5.1.121	10.5.1.121

4.8.6 Jabber Guest Servers

Cisco Jabber Guest is a consumer to business (C2B) solution that extends the reach of Cisco's enterprise telephony to people outside of a corporate firewall who do not have phones registered with Cisco Unified Communications Manager.

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

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

< No records found >

4.9 Dial Plan

This section shows the structure of the Dial Plan. The Dial Plan determines the aliases assigned to the endpoints, and the way in which the VCSs are neighboured together. The choice of solution will depend on the complexity of the system. The section is divided into:

- Configuration
- Transforms
- Search Rules
- Policy Services

4.9.1 Configuration

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

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

Dial Plan Configuration	
Configuration	
Calls to unknown IP addresses	Direct
Fallback alias	test

4.9.2 Transforms

Transforms are used to modify the alias in a search request if it matches certain criteria. An alias can be transformed 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.
- 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.

Transforms						
Priority	**State**	**Description**	**Pattern**	**Type**	**Behavior**	**Replace**
1	Enabled	Transform1	Transform1	Prefix	Strip	
2	Enabled	Transform2	Transform2	Prefix	Replace	8856445XX

4.9.3 Search Rules

The Search rules section contains configuration showing how the VCS routes incoming search requests to the appropriate target zones (including the Local Zone) or policy services.

Search Rules	
Name	**Details**
LocalZoneMatch	**Configuration**
	Rule name: LocalZoneMatch
	Description: Default rule: queries the Local Zone for any alias
	Priority: 50
	Protocol: Any
	Source: Any
	Request must be authenticated: No
	Mode: AnyAlias
	On successful match: Continue
	Target: LocalZone
	State: Enabled
CEtcp-10.5.1.120	**Configuration**
	Rule name: CEtcp-10.5.1.120
	Description: CE for UCM TCP 10.5.1.120
	Priority: 45
	Protocol: SIP
	Source: Any
	Request must be authenticated: No
	Mode: AliasPatternMatch
	Pattern type: Prefix
	Pattern string: 10.5.1.120;transport=TCP
	Pattern behavior: Leave
	On successful match: Stop

Search Rules		
Name	**Details**	
	Target	CEtcp-10.5.1.120
	State	Enabled
CEtcp-10.5.1.150	**Configuration**	
	Rule name	CEtcp-10.5.1.150
	Description	CE for UCM TCP 10.5.1.150
	Priority	45
	Protocol	SIP
	Source	Any
	Request must be authenticated	No
	Mode	AliasPatternMatch
	Pattern type	Prefix
	Pattern string	10.5.1.150;transport=TCP
	Pattern behavior	Leave
	On successful match	Stop
	Target	CEtcp-10.5.1.150
	State	Enabled
search rule1	**Configuration**	
	Rule name	search rule1
	Description	Desc search rule1
	Priority	100
	Protocol	Any
	Source	Any
	Request must be authenticated	No
	Mode	AnyAlias
	On successful match	Continue
	Target	Zone1234567
	State	Enabled

4.9.4 Policy Services

This section shows the media encryption policy settings which enables one to selectively add or remove media encryption capabilities for SIP calls flowing through the VCS. The system is configured such that, for example, all traffic arriving or leaving a VCS Expressway from the public internet is encrypted, but is unencrypted when in private network.

Policy Services		
Name	**Details**	
Policy service 1	**Configuration**	
	Name	Policy service 1
	Description	Desc policy service1
	Protocol	HTTPS
	Certificate verification mode	Off
	HTTPS certificate revocation list (CRL) checking	Off
	Server 1 address	10.5.1.120
	Server 2 address	
	Server 3 address	
	Path	/sp/path.xml
	Status path	status
	Username	admin
	Default CPL	<reject status='504' reason='Policy Service Unavailable'/>

4.10 Bandwidth

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. The section includes:

- Configuration
- Links
- Pipes

4.10.1 Configuration

The Bandwidth configuration is used to specify how the VCS behaves in situations when it receives a call with no bandwidth specified, and when it receives a call that requests more bandwidth than is currently available.

Bandwidth Configuration	
Configuration	
Default call bandwidth (kbps)	384
Downspeed per call mode	On
Downspeed total mode	On

4.10.2 Links

Links connect local subzones with other subzones and zones. For a call to take place, the endpoints involved must each reside in subzones or zones that have a link between them. The link does not need to be direct; the two endpoints may be linked via one or more intermediary subzones.

Links are used to calculate how a call is routed over the network and therefore which zones and subzones are involved and how much bandwidth is available. If multiple routes are possible, your VCS will perform the bandwidth calculations using the one with the fewest links.

Links				
Name	**Node1**	**Node2**	**Pipe1**	**Pipe2**
DefaultSZtoTraversalSZ	DefaultSubZone	TraversalSubZone		
SubZone002ToTraversalSZ	subzone2	TraversalSubZone		
Zone002ToDefaultSZ	zone2	DefaultSubZone		
Zone002ToTraversalSZ	zone2	TraversalSubZone		
Zone003ToDefaultSZ	CEtcp-10.5.1.120	DefaultSubZone		Pipe1
Zone003ToTraversalSZ	CEtcp-10.5.1.120	TraversalSubZone		
Zone004ToDefaultSZ	CEtcp-10.5.1.150	DefaultSubZone		
Zone004ToTraversalSZ	CEtcp-10.5.1.150	TraversalSubZone		
Zone005ToDefaultSZ	ZoneDNSyo	DefaultSubZone		
Zone005ToTraversalSZ	ZoneDNSyo	TraversalSubZone		
Zone006ToTraversalSZ	ZONEtravclient	TraversalSubZone		
DefaultSZtoDefaultZ	DefaultSubZone	DefaultZone		
Zone007ToTraversalSZ	UCTraversalZone	TraversalSubZone		
DefaultSZtoClusterSZ	DefaultSubZone	ClusterSubZone		
TraversalSZtoDefaultZ	TraversalSubZone	DefaultZone		
Zone001ToDefaultSZ	Zone1234567	DefaultSubZone		
Zone001ToTraversalSZ	Zone1234567	TraversalSubZone		
SubZone001ToDefaultSZ	subzone1	DefaultSubZone		
SubZone001ToTraversalSZ	subzone1	TraversalSubZone		
SubZone002ToDefaultSZ	subzone2	DefaultSubZone		

4.10.3 Pipes

Pipes are used to control the amount of bandwidth used on calls between specific subzones and zones. The limits can be applied to the total concurrent bandwidth used at any one time, or to the bandwidth used by any individual call.

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

Pipes	
Name	**Details**
Pipe1	**Configuration**
	Name: Pipe1
	Total Bandwidth Available
	Bandwidth restriction: Limited
	Total bandwidth limit (kbps): 5444332
	Calls Through This Pipe
	Bandwidth restriction: NoBandwidth
	Per call bandwidth limit (kbps): 1920

4.11 Call Policy

This section contains the rules used to control which calls are allowed, which calls are rejected, and which calls are to be redirected to a different destination. These rules are known as Call Policy (or Administrator Policy).

If Call Policy is enabled and has been configured, each time a call is made the VCS will execute the policy in order to decide, based on the source and destination of the call, whether to:

- Proxy the call to its original destination
- Redirect the call to a different destination or set of destinations
- Reject the call

4.11.1 Configuration

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

- Local CPL: uses locally-defined Call Policy.
- Policy service: uses an external policy service.
- Off: Call Policy is not in use.

Configuration	
Call Policy mode	Local CPL

4.12 Traversal

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

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

This section shows settings for:

- Ports
- TURN
- Endpoints

4.12.1 Ports

The Expressway-E has specific listening ports used for firewall traversal. The correct ports must be set on the Expressway-E, traversal client and firewall in order for connections to be permitted. Rules must be set on your firewall to allow connections to these ports. In most cases the default ports should be used.

The following ports are configured:

Ports
Demultiplexing Ports

Use configured demultiplexing ports	
Call Signaling Ports	
H.323 Assent call signaling port	
H.323 H.460.18 call signaling port	

4.12.2 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.

TURN relay services are only available on the Expressway-E. To use TURN services you need the TURN Relay option key (this controls the number of TURN relays that can be simultaneously allocated by the TURN server). This section lists the Expressway-E's TURN settings.

TURN	
Server	
TURN services	
TURN requests port	
Authentication realm	
Media port range start	
Media port range end	

4.12.3 Locally registered endpoints

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

The following are the settings for endpoints to register.

Locally Registered Endpoints	
Configuration	
H.323 Assent mode	
H.460.18 mode	
H.460.19 demultiplexing mode	
H.323 preference	
UDP probe retry interval	
UDP probe retry count	
UDP probe keep alive interval	
TCP probe retry interval	
TCP probe retry count	
TCP probe keep alive interval	

5 Applications

This section provides information about each of the additional services that are available under the Applications menu of the VCS. The report shows:

- Conference Factory
- Presence
- FindMe

5.1 Conference Factory

The Conference Factory shows whether the Conference Factory application is enabled and disabled, and the alias and template it uses.

The Conference Factory application allows the 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).

Conference Factory	
Configuration	
Mode	Off
Alias	
Template	
Number range start	1
Number range end	65535

5.2 Presence

Presence is the ability of endpoints to provide information to other users about their current status - such as whether they are offline, online, or in a call. Any entity which provides presence information, or about whom presence information can be requested, is known as a presentity. Presentities publish information about their own presence status, and also subscribe to the information being published by other presentities and FindMe users.

Endpoints that support presence, such as Jabber Video, can publish their own status information. The VCS can also provide basic presence information on behalf of endpoints that do not support presence, including H.323 endpoints, as long as they have registered with an alias in the form of a URI.

Presence	
PUA	
SIP SIMPLE Presence user agent	Off
Default published status for registered endpoints	Online
Presence Server	
SIP SIMPLE Presence server	Off

5.3 FindMe

FindMe is a form of User Policy, which is the set of rules that determines what happens to a call for a particular user or group when it is received by the Expressway.

The FindMe feature lets you assign a single FindMe ID to individuals or teams in your enterprise. By logging into their FindMe account, users can set up a list of locations such as "at home" or "in the office" and associate their devices with those locations. They can then specify which devices are called when their FindMe ID is dialled, and what happens if those devices are busy or go unanswered. Each user can specify up to 15 devices and 10 locations.

FindMe	
FindMe mode	Off

6 Users

This section provides information about how to configure administrator and FindMe user accounts, and how to display the details of all active administrator and FindMe sessions. This section shows the following:

- Password Security
- Administrator Accounts
- Administrator Groups
- LDAP Configuration

6.1 Password Security

The Password security controls whether or not local administrator account passwords must meet a minimum level of complexity before they are accepted.

If Enforce Strict Passwords is set to On, all subsequently configured local administrator account passwords must conform to the following rules for what constitutes a strict password.

Password Security	
Strict Passwords	
Enforce strict passwords	On

6.2 Administrator Accounts

The Administrator Accounts section lists all the local administrator accounts on the VCS.

In general, local administrator accounts are used to access the VCS on its web interface or API interface, but are not permitted to access the CLI.

Administrator Accounts		
Name	**Details**	
admin	State	Enabled
	Web access	On
	API access	On
	Password Reset Required	Off

6.3 Administrator Groups

The Administrator Groups section lists all the administrator groups that have been configured on the VCS, and allows to add, edit and delete groups.

Administrator groups only apply if remote account authentication is enabled.

When logged in to the VCS web interface, the credentials are authenticated against the remote directory service and assigned access rights associated with the group to which one belongs. If the administrator account belongs to more than one group, the highest level permission is assigned.

Administrator Groups		
Name	**Details**	
AdminGroup1	State	Enabled
	Web access	On
	API access	On

6.4 LDAP Configuration

The LDAP configuration is used to configure an LDAP connection to a remote directory service for administrator account authentication. It can also provide user account authentication if using FindMe without Cisco TMS.

LDAP Configuration	
Remote Account Authentication	
Administrator authentication source	Local
FindMe authentication source	Local

7 Maintenance

The Maintenance section of the report contains:

- Logging Configuration
- Maintenance Mode
- Language
- Diagnostics

7.1 Logging Configuration

The VCS provides syslogging features for troubleshooting and auditing purposes.

The Event Log is a rotating local log that records information about such things as calls, registrations, and messages sent and received.

Logging Configuration	
Event Logging	
Local event log verbosity	1
Media statistics	off

Call Detail Records (CDR)	off
System Metrics	
System metrics collection	off
Collection interval (seconds)	60
Collection server address	
Collection server port	25826

7.2 Maintenance Mode

Maintenance mode is typically used to upgrade or take out of service a VCS peer that is part of a cluster. It allows the other cluster peers to continue to operate normally while the peer that is in maintenance mode is upgraded or serviced.

Maintenance Mode	
Maintenance mode	Off

7.3 Language

The Language controls which language is used for text displayed in the web user interface. The default language used on the web interface.

Language	
Default system language	en_US - American English

7.4 Diagnostics

This section shows diagnostic log configuration.

7.4.1 Incident Reporting

The incident reporting feature of the VCS automatically saves information about critical system issues such as application failures.

7.4.1.1 Configuration

This section shows the Incident Reporting settings.

Incident Reporting Configuration	
Configuration	
Incident reports sending mode	off
Incident reports URL	https://cc-reports.cisco.com/submitapplicationerror/
Contact email address	
Proxy server	
Create core dumps	On

7.4.2 Advanced

This section shows settings for the following:

- Network Log Configuration
- Support Log Configuration

7.4.2.1 Network Log Configuration

This section shows the Network Log configuration used to configure the log levels for the range of Network Log message modules.

Network Log Configuration	
Name	**Level**
network	INFO
network.ashell	INFO

Network Log Configuration	
Name	**Level**
network.authentication	INFO
network.axl	INFO
network.cpl	INFO
network.dns	INFO
network.h323	INFO
network.http	INFO
network.http.edgeconfigprovisioning	INFO
network.http.trafficserver	INFO
network.ldap	INFO
network.mediarouting	INFO
network.rpcnetlogon	INFO
network.search	INFO
network.sip	INFO
network.sourcealiasrewriting	INFO
network.tcp	INFO
network.ucxn	INFO
network.uds	INFO
network.unknown	INFO

7.4.2.2 Support Log Configuration

This section shows Support Log configuration used to configure the log levels for the range of Support Log message modules.

Support Log Configuration	
Name	**Level**
developer	INFO
developer.CollaborationEdge	INFO
developer.CollaborationEdge.twisted	INFO
developer.CrashReporter.twisted	INFO
developer.DomMngmnt.twisted	INFO
developer.InstallWizard.twisted	INFO
developer.Management	INFO
developer.Management.twisted	INFO
developer.Phonebook.twisted	INFO
developer.Provisioning.twisted	INFO
developer.Supervisor.twisted	INFO
developer.abstraction	INFO
developer.addresschooser	INFO
developer.adminusermanager	INFO
developer.adminusermanager.accessconfwriter	INFO
developer.adminusermanager.consolegidswriter	INFO
developer.alarmmanager	INFO
developer.alternates.config	INFO
developer.application	INFO
developer.applicationmanager	INFO
developer.applicationmanager.livenessmonitor	INFO
developer.applicationmanager.livenessmonitor.allowedmethods	INFO
developer.applicationmanager.policy	INFO
developer.applicationmanager.policyconfigurator	INFO
developer.applications	INFO

Support Log Configuration	
Name	**Level**
developer.applications.linuxmanager	INFO
developer.appmanager.callhistory	INFO
developer.appmanager.registrationhistory	INFO
developer.ashell	INFO
developer.ashell.cdb	INFO
developer.ashell.cuil	INFO
developer.ashell.plugin	INFO
developer.ashell.twisted	INFO
developer.auth	INFO
developer.auth.digest.cache	INFO
developer.auth.digest.limitedcache	INFO
developer.auth.digestauth	INFO
developer.auth.noncemanager.ntlmauthmanager	INFO
developer.auth.noncemanager.sip	INFO
developer.auth.noncemanager.stun	INFO
developer.auth.ntlm	INFO
developer.authentication.oauth	INFO
developer.b2bua	INFO
developer.b2bua.b2buametrics	INFO
developer.b2bua.b2buametrics.manager	INFO
developer.b2bua.configuration	INFO
developer.b2bua.configuration.nettle	INFO
developer.b2bua.launcher	INFO
developer.bandwidth.bandwidthmgr	INFO
developer.bandwidth.infosharingprotocol	INFO
developer.call	INFO
developer.call.callcounter	INFO
developer.callserialnumber	INFO
developer.callusagemanager	INFO
developer.callusagemanager.callstatus	INFO
developer.cdap.framework	INFO
developer.cdap.provider.ServiceRecordsProvider	INFO
developer.cdbconfigmgr	INFO
developer.cdbstatussync	INFO
developer.cdbstatussync.callhistoryconverter	INFO
developer.cdbstatussync.callstatusconverter	INFO
developer.cdbstatussync.event	INFO
developer.cdbstatussync.event.httpresponseeventdispatcher	INFO
developer.cdbstatussync.ivycallhistoryconverter	INFO
developer.cdbstatussync.ivycallstatusconverter	INFO
developer.cdbstatussync.queue	INFO
developer.cdbstatussync.queue.cdbeventqueueeventdispatcher	INFO
developer.cdbstatussync.registrationhistoryconverter	INFO
developer.cdbstatussync.registrationstatusconverter	INFO
developer.cdbtable.cdb.accountSecurityConfiguration	INFO
developer.cdbtable.cdb.acmeProviders	INFO
developer.cdbtable.cdb.adminAccountConfiguration	INFO
developer.cdbtable.cdb.administrationInterfaceConfiguration	INFO
developer.cdbtable.cdb.alarmStatus	INFO
developer.cdbtable.cdb.alternatesConfiguration	INFO

Support Log Configuration	
Name	**Level**
developer.cdbtable.cdb.alternatesMasterConfiguration	INFO
developer.cdbtable.cdb.authenticationCredentialConfiguration	INFO
developer.cdbtable.cdb.authenticationH350Configuration	INFO
developer.cdbtable.cdb.authorizedkeys	INFO
developer.cdbtable.cdb.authzkeys	INFO
developer.cdbtable.cdb.b2buaICEMetrics	INFO
developer.cdbtable.cdb.b2buaListenerPermissionConfiguration	INFO
developer.cdbtable.cdb.b2buaPresenceRelayConfiguration	INFO
developer.cdbtable.cdb.b2buaServiceConfiguration	INFO
developer.cdbtable.cdb.b2buaServiceStatus	INFO
developer.cdbtable.cdb.b2buaTranscoderPermissionConfiguration	INFO
developer.cdbtable.cdb.b2buaTranscoderResourceUseConfiguration	INFO
developer.cdbtable.cdb.b2buaTurnServerConfiguration	INFO
developer.cdbtable.cdb.bootstrapPublic	INFO
developer.cdbtable.cdb.cafeBlobConfiguration	INFO
developer.cdbtable.cdb.cafeStaticConfiguration	INFO
developer.cdbtable.cdb.callStatus	INFO
developer.cdbtable.cdb.cbaConfiguration	INFO
developer.cdbtable.cdb.cipherConfiguration	INFO
developer.cdbtable.cdb.cloudDomainsConfiguration	INFO
developer.cdbtable.cdb.clusterConfiguration	INFO
developer.cdbtable.cdb.clusterPeerConfiguration	INFO
developer.cdbtable.cdb.clusterPeerStatus	INFO
developer.cdbtable.cdb.clusterStatus	INFO
developer.cdbtable.cdb.cmsAddCommand	INFO
developer.cdbtable.cdb.cmsAddCommandResult	INFO
developer.cdbtable.cdb.cucmCerts	INFO
developer.cdbtable.cdb.cucmConfigAddCommand	INFO
developer.cdbtable.cdb.cucmConfigAddCommandResult	INFO
developer.cdbtable.cdb.cucmHttpProxyConfiguration	INFO
developer.cdbtable.cdb.cucmNodes	INFO
developer.cdbtable.cdb.cucmTftp	INFO
developer.cdbtable.cdb.defaultZoneTlsConfiguration	INFO
developer.cdbtable.cdb.directorypolicyclusterconfiguration	INFO
developer.cdbtable.cdb.directorypolicyfilterconfiguration	INFO
developer.cdbtable.cdb.directorypolicyhomeclusterconfiguration	INFO
developer.cdbtable.cdb.directorypolicyserviceshomeclusterconfiguration	INFO
developer.cdbtable.cdb.directorypolicysubnethomeclusterconfiguration	INFO
developer.cdbtable.cdb.dnsConfiguration	INFO
developer.cdbtable.cdb.dnsPerDomainServerConfiguration	INFO
developer.cdbtable.cdb.dnsServerConfiguration	INFO
developer.cdbtable.cdb.edgeCmsServerAddresses	INFO
developer.cdbtable.cdb.edgeCmsServerConfig	INFO
developer.cdbtable.cdb.edgeCmsServerStatus	INFO
developer.cdbtable.cdb.edgeConfigProvisioningCUCMConfiguration	INFO
developer.cdbtable.cdb.edgeConfigProvisioningCUCMDiscoveryConfiguration	INFO
developer.cdbtable.cdb.edgeConfigProvisioningCUPDiscoveryConfiguration	INFO
developer.cdbtable.cdb.edgeConfigProvisioningServerConfiguration	INFO
developer.cdbtable.cdb.edgeDeploymentConfig	INFO
developer.cdbtable.cdb.edgeDomainConfig	INFO

Support Log Configuration	
Name	**Level**
developer.cdbtable.cdb.edgeDomainInfo	INFO
developer.cdbtable.cdb.edgeManagement	INFO
developer.cdbtable.cdb.edgeSsoStatus	INFO
developer.cdbtable.cdb.errorReportConfiguration	INFO
developer.cdbtable.cdb.externalManagerConfiguration	INFO
developer.cdbtable.cdb.fail2banBannedAddress	INFO
developer.cdbtable.cdb.fail2banCommand	INFO
developer.cdbtable.cdb.fail2banCommandResult	INFO
developer.cdbtable.cdb.fail2banGlobalAllowList	INFO
developer.cdbtable.cdb.fail2banJailConfiguration	INFO
developer.cdbtable.cdb.fail2banJailStatus	INFO
developer.cdbtable.cdb.fail2banStatus	INFO
developer.cdbtable.cdb.findmeDeviceConfiguration	INFO
developer.cdbtable.cdb.findmeLocationConfiguration	INFO
developer.cdbtable.cdb.findmeLocationDeviceConfiguration	INFO
developer.cdbtable.cdb.findmeUserConfiguration	INFO
developer.cdbtable.cdb.fipsStatus	INFO
developer.cdbtable.cdb.firewallCommand	INFO
developer.cdbtable.cdb.forwardProxyConfiguration	INFO
developer.cdbtable.cdb.globalPrivate	INFO
developer.cdbtable.cdb.h323Configuration	INFO
developer.cdbtable.cdb.hardwareStatus	INFO
developer.cdbtable.cdb.hosts	INFO
developer.cdbtable.cdb.httpAllowListAuto	INFO
developer.cdbtable.cdb.httpAllowListControl	INFO
developer.cdbtable.cdb.httpAllowListManual	INFO
developer.cdbtable.cdb.httpAllowListRuleAddCommand	INFO
developer.cdbtable.cdb.httpAllowListRuleAddCommandResult	INFO
developer.cdbtable.cdb.hybridServicesLoggerConfiguration	INFO
developer.cdbtable.cdb.iptablesAcceptedRuleStatus	INFO
developer.cdbtable.cdb.iptablesFileConfiguration	INFO
developer.cdbtable.cdb.iptablesRuleConfiguration	INFO
developer.cdbtable.cdb.iptablesRuleStatus	INFO
developer.cdbtable.cdb.iptablesStateStatus	INFO
developer.cdbtable.cdb.knownhosts	INFO
developer.cdbtable.cdb.licenseManagerLicensePoolStatus	INFO
developer.cdbtable.cdb.licensePoolLimitsStatus	INFO
developer.cdbtable.cdb.loginLDAPConfiguration	INFO
developer.cdbtable.cdb.networkConfiguration	INFO
developer.cdbtable.cdb.networkInterfaceConfiguration	INFO
developer.cdbtable.cdb.networkInterfaceCountersStatus	INFO
developer.cdbtable.cdb.networkInterfaceStatus	INFO
developer.cdbtable.cdb.networkLimitsCommand	INFO
developer.cdbtable.cdb.networkLimitsCommandResult	INFO
developer.cdbtable.cdb.networkRouteConfiguration	INFO
developer.cdbtable.cdb.ntpKeyPassword	INFO
developer.cdbtable.cdb.ntpServerConfiguration	INFO
developer.cdbtable.cdb.ntpServerStatus	INFO
developer.cdbtable.cdb.oauthValidCacheConfiguration	INFO
developer.cdbtable.cdb.peerResolverStatus	INFO

Support Log Configuration	
Name	**Level**
developer.cdbtable.cdb.phonebookContactMethodConfiguration	INFO
developer.cdbtable.cdb.phonebookEntryConfiguration	INFO
developer.cdbtable.cdb.phonebookFolderConfiguration	INFO
developer.cdbtable.cdb.phonebookServerStatus	INFO
developer.cdbtable.cdb.phonebookUserAccessConfiguration	INFO
developer.cdbtable.cdb.protocolQoS	INFO
developer.cdbtable.cdb.provisioningServerStatus	INFO
developer.cdbtable.cdb.provisioningServiceConfiguration	INFO
developer.cdbtable.cdb.provisioningServiceStatus	INFO
developer.cdbtable.cdb.provisioningSettingsConfiguration	INFO
developer.cdbtable.cdb.registrationStatus	INFO
developer.cdbtable.cdb.resourceUsageStatus	INFO
developer.cdbtable.cdb.samlIdPMetaDataConfiguration	INFO
developer.cdbtable.cdb.samlMetaDataConfiguration	INFO
developer.cdbtable.cdb.samlMetaDataExportedConfiguration	INFO
developer.cdbtable.cdb.serviceConfiguration	INFO
developer.cdbtable.cdb.serviceselectConfiguration	INFO
developer.cdbtable.cdb.sessionLimitConfiguration	INFO
developer.cdbtable.cdb.shardedPrivate	INFO
developer.cdbtable.cdb.sipConfiguration	INFO
developer.cdbtable.cdb.sipDomainConfiguration	INFO
developer.cdbtable.cdb.sipParamDbConfiguration	INFO
developer.cdbtable.cdb.sipservice	INFO
developer.cdbtable.cdb.sipservicedomain	INFO
developer.cdbtable.cdb.sipservicezone	INFO
developer.cdbtable.cdb.snmpConfiguration	INFO
developer.cdbtable.cdb.systemConfiguration	INFO
developer.cdbtable.cdb.systemScale	INFO
developer.cdbtable.cdb.systemStatus	INFO
developer.cdbtable.cdb.timeConfiguration	INFO
developer.cdbtable.cdb.timeStatus	INFO
developer.cdbtable.cdb.tlpStatus	INFO
developer.cdbtable.cdb.tmsdiscovery	INFO
developer.cdbtable.cdb.ucaddresses	INFO
developer.cdbtable.cdb.ucnames	INFO
developer.cdbtable.cdb.ucxnConfigAddCommand	INFO
developer.cdbtable.cdb.ucxnConfigAddCommandResult	INFO
developer.cdbtable.cdb.ucxnConfiguration	INFO
developer.cdbtable.cdb.ucxnServers	INFO
developer.cdbtable.cdb.userGroupConfiguration	INFO
developer.cdbtable.cdb.userPreferenceGroupConfiguration	INFO
developer.cdbtable.cdb.userPreferenceTemplateConfiguration	INFO
developer.cdbtable.cdb.userPreferenceUserConfiguration	INFO
developer.cdbtable.cdb.vcsConfiguration	INFO
developer.cdbtable.cdb.vcsConfigurationBrief	INFO
developer.cdbtable.cdb.xcpCerts	INFO
developer.cdbtable.cdb.xcpConfiguration	INFO
developer.cdbtable.cdb.xcpDomains	INFO
developer.cdbtable.cdb.xcpR2RConfigExpressway	INFO
developer.cdbtable.cdb.xcpR2RConfiguration	INFO

Support Log Configuration	
Name	**Level**
developer.cdbtable.cdb.xcpS2SConfiguration	INFO
developer.cdbtable.cdb.xcpTcaliases	INFO
developer.cdbtable.cdb.xmppdiscoveryCommand	INFO
developer.cdbtable.cdb.xmppdiscoveryCommandResult	INFO
developer.certchecker	INFO
developer.certificate.verifier	INFO
developer.cipher.configmonitor	INFO
developer.clientedge.conn	INFO
developer.clouddomaindb	INFO
developer.cluster.config	INFO
developer.clusterdb.alternatesmanager	INFO
developer.clusterdb.appmanager	INFO
developer.clusterdb.bulkbuffer	INFO
developer.clusterdb.bulkcdb	INFO
developer.clusterdb.bulkrest	INFO
developer.clusterdb.cdb	INFO
developer.clusterdb.cdb.mnesia	INFO
developer.clusterdb.cdb.msgtrace	INFO
developer.clusterdb.clustermanager	INFO
developer.clusterdb.clusterstatus	INFO
developer.clusterdb.clusterstatus.ratelimit	INFO
developer.clusterdb.earlydb	INFO
developer.clusterdb.earlydb.tls	INFO
developer.clusterdb.inotify	INFO
developer.clusterdb.optionkey	INFO
developer.clusterdb.peernameresolver	INFO
developer.clusterdb.registrar	INFO
developer.clusterdb.restapi	INFO
developer.clusterpeerstatus	INFO
developer.clusterstatus	INFO
developer.clusterstatus.twisted	INFO
developer.cnfigsys	INFO
developer.command	INFO
developer.commandhandler	INFO
developer.commandmanager	INFO
developer.commandmanager.b2buadial	INFO
developer.commandmanager.b2buadisconnect	INFO
developer.commandmanager.sipservicecheck	INFO
developer.config	INFO
developer.config.interestregistrar	INFO
developer.config.validator	INFO
developer.crashmonitord	INFO
developer.crashreport	INFO
developer.credentialmanager	INFO
developer.credentialmanager.h350	INFO
developer.credentialmanager.ldap	INFO
developer.credentialmanager.oauthinspector	INFO
developer.credentialmanager.oauthtokenmanager	INFO
developer.credentialmanager.oauthvalidator	INFO
developer.credentialmanager.service	INFO

Support Log Configuration	
Name	**Level**
developer.credentialmanager.service.server	INFO
developer.credentialmanager.twisted	INFO
developer.cuil	INFO
developer.curlservice.fsm	INFO
developer.curlservice.fsm.impl	INFO
developer.cvs	INFO
developer.cvs.certificate_dao	INFO
developer.cvs.certificate_store	INFO
developer.cvs.server	INFO
developer.cvs.twisted	INFO
developer.cvs.verifier	INFO
developer.daemonprivileges	INFO
developer.dbusmgr	INFO
developer.defaultpasswordcheck.twisted	INFO
developer.diagnostics	INFO
developer.diagnostics.alarmmanager	INFO
developer.diagnostics.alarmstartup	INFO
developer.diagnostics.asyncalarmmanager	INFO
developer.diagnostics.eventmanager	INFO
developer.diagnostics.eventmanagerbackend	INFO
developer.directorypolicy	INFO
developer.directorypolicy.admin	INFO
developer.directorypolicy.basepolicy	INFO
developer.directorypolicy.call	INFO
developer.directorypolicy.cdb	INFO
developer.directorypolicy.registration	INFO
developer.directorypolicy.server	INFO
developer.directorypolicy.service	INFO
developer.directorypolicy.services	INFO
developer.directorypolicy.subnet	INFO
developer.directorypolicy.twisted	INFO
developer.directorypolicy.user	INFO
developer.directorypolicy.vcsconfig	INFO
developer.dns.uriresolver	INFO
developer.domain_management	INFO
developer.domaindb	INFO
developer.edgeconfigprovisioning	INFO
developer.edgeconfigprovisioning.cache	INFO
developer.edgeconfigprovisioning.server	INFO
developer.edgeconfigprovisioning.ucnodes	INFO
developer.edgeconfigprovisioning.utils	INFO
developer.edgemanager	INFO
developer.edgemanager.cmsdata	INFO
developer.edgemanager.conn	INFO
developer.edgemanager.domaindata	INFO
developer.edgemanager.s2sdata	INFO
developer.edgemanager.startupcheck	INFO
developer.edgemanager.xcpdata	INFO
developer.extappstatus	INFO
developer.externalmanager	INFO

Support Log Configuration	
Name	**Level**
developer.externalmanager.importer	INFO
developer.externalmanager.parser	INFO
developer.externalmanager.processor	INFO
developer.externalmanager.processor.devicerepository	INFO
developer.externalmanager.processor.findme	INFO
developer.externalmanager.processor.phonebook	INFO
developer.externalmanager.processor.userpreference	INFO
developer.externalmanager.tlswrapper	INFO
developer.fdmonitor	INFO
developer.fips.configmonitor	INFO
developer.framework.applicationobjectcontroller	INFO
developer.framework.fdmonitor	INFO
developer.framework.interfacebroker	INFO
developer.framework.serviceobjectcontroller	INFO
developer.framework.threadeddispatcher	INFO
developer.fsm	INFO
developer.fsm.assentclient	INFO
developer.fsm.assentserver	INFO
developer.fsm.audiomodule	INFO
developer.fsm.bluereader	INFO
developer.fsm.cfg	INFO
developer.fsm.com	INFO
developer.fsm.cuilfsm	INFO
developer.fsm.curlservicefsm	INFO
developer.fsm.diffieh	INFO
developer.fsm.distpar	INFO
developer.fsm.dns	INFO
developer.fsm.dnsresponsemgrfsm	INFO
developer.fsm.dport	INFO
developer.fsm.extappstatus	INFO
developer.fsm.externalclient	INFO
developer.fsm.extmng	INFO
developer.fsm.fal	INFO
developer.fsm.fsm_timer	INFO
developer.fsm.fsmsys_fsm	INFO
developer.fsm.fsmwatchdog	INFO
developer.fsm.fsmwrapper	INFO
developer.fsm.gkh245route	INFO
developer.fsm.gkq931route	INFO
developer.fsm.gkras	INFO
developer.fsm.gktest	INFO
developer.fsm.h110ctrl	INFO
developer.fsm.h245leg	INFO
developer.fsm.h245server	INFO
developer.fsm.h323connectionmgrfsm	INFO
developer.fsm.h323legfsm	INFO
developer.fsm.h323msgdsp	INFO
developer.fsm.h323sys	INFO
developer.fsm.h460client	INFO
developer.fsm.httpfeed	INFO

Support Log Configuration	
Name	**Level**
developer.fsm.httpfsm	INFO
developer.fsm.iir	INFO
developer.fsm.internalclient	INFO
developer.fsm.l1chip	INFO
developer.fsm.lcdreader	INFO
developer.fsm.lincfg	INFO
developer.fsm.logger	INFO
developer.fsm.makedebugstr_func	INFO
developer.fsm.mcaspmsg	INFO
developer.fsm.mcaspraw	INFO
developer.fsm.mediahalfsfsm	INFO
developer.fsm.mediasessiontestfsm	INFO
developer.fsm.mrconfigurator	INFO
developer.fsm.mrmgr	INFO
developer.fsm.mrtest	INFO
developer.fsm.mrtomsfsm	INFO
developer.fsm.msmgr	INFO
developer.fsm.oakcommandhandler	INFO
developer.fsm.oaktestfsm	INFO
developer.fsm.operlog	INFO
developer.fsm.par	INFO
developer.fsm.pci_if	INFO
developer.fsm.pool_spec	INFO
developer.fsm.prichip	INFO
developer.fsm.pridchan	INFO
developer.fsm.q931leg	INFO
developer.fsm.q931server	INFO
developer.fsm.q_cp	INFO
developer.fsm.rs366ll	INFO
developer.fsm.sgim	INFO
developer.fsm.shmem_arm	INFO
developer.fsm.shmem_dsp	INFO
developer.fsm.singlesocket	INFO
developer.fsm.sipmsgdsp	INFO
developer.fsm.sipproxylegfsm	INFO
developer.fsm.sipproxymsgdspfsm	INFO
developer.fsm.sipserviceserverfsm	INFO
developer.fsm.siptrans	INFO
developer.fsm.siptrav	INFO
developer.fsm.siptravtest	INFO
developer.fsm.siptrlay	INFO
developer.fsm.siptrnsp	INFO
developer.fsm.socketpair	INFO
developer.fsm.sockhandler	INFO
developer.fsm.sourcealiasrewriterfsm	INFO
developer.fsm.system	INFO
developer.fsm.telnet	INFO
developer.fsm.test_spec	INFO
developer.fsm.timerlist	INFO
developer.fsm.transitlocationnodefsm	INFO

Support Log Configuration	
Name	**Level**
developer.fsm.traversalclientfsm	INFO
developer.fsm.turnsrv	INFO
developer.fsm.turntestclient	INFO
developer.fsm.uhpi_dsp	INFO
developer.fsm.uhpi_host	INFO
developer.fsm.v35ll	INFO
developer.fsm.vidses	INFO
developer.fsm.web	INFO
developer.fsm.winbindservicefsm	INFO
developer.fsm.xacli	INFO
developer.gkh323stack	INFO
developer.globalstatistics	INFO
developer.h323.connectionmgr	INFO
developer.h323.h225connection	INFO
developer.h323.h245connection	INFO
developer.h323.lib.retrans	INFO
developer.h323.listener	INFO
developer.h323.locationresponsemgr	INFO
developer.h323.msgdsp	INFO
developer.h323.traversal.traversalclient	INFO
developer.http	INFO
developer.httpclient	INFO
developer.httpclientcurl.httpconnectionpool	INFO
developer.httpclientcurl.httprequest	INFO
developer.httpclientcurl.httpresponsenoop	INFO
developer.installwizard	INFO
developer.installwizard.sshd	INFO
developer.iwf	INFO
developer.license	INFO
developer.licensemanager.service	INFO
developer.licensemanager.service.licensepool	INFO
developer.licensemanager.service.manager	INFO
developer.licensemanager.service.server	INFO
developer.licensemanager.service.utils	INFO
developer.licensemanager.twisted	INFO
developer.linux.packages	INFO
developer.management	INFO
developer.management.accountsecuritymanager	INFO
developer.management.acmealarmmanager	INFO
developer.management.acmeautorenew	INFO
developer.management.acmecertbotutils	INFO
developer.management.acmedeletependingcertcommand	INFO
developer.management.acmedeploy	INFO
developer.management.acmegetpendingcertcommand	INFO
developer.management.acmeproviders	INFO
developer.management.acmereset	INFO
developer.management.acmerevoke	INFO
developer.management.acmesettingsread	INFO
developer.management.acmesettingswrite	INFO
developer.management.acmesigncommand	INFO

Support Log Configuration	
Name	**Level**
developer.management.acmestate	INFO
developer.management.acmesyncmanager	INFO
developer.management.adminusermanager	INFO
developer.management.alarmledmanager	INFO
developer.management.alarmotdmanager	INFO
developer.management.apache	INFO
developer.management.callusagenotifier	INFO
developer.management.certs	INFO
developer.management.ciphermanager	INFO
developer.management.cms	INFO
developer.management.commandcleanup	INFO
developer.management.commandline	INFO
developer.management.connectivitytest	INFO
developer.management.crlupdatermanager	INFO
developer.management.cucmconfig	INFO
developer.management.cucmconfig.zoneconfig	INFO
developer.management.databasemanager	INFO
developer.management.dbusmanager	INFO
developer.management.diagnosticsmanager	INFO
developer.management.dnslookup	INFO
developer.management.domainaggregator	INFO
developer.management.domaincerts	INFO
developer.management.edgedeploymentsmanager	INFO
developer.management.fail2ban	INFO
developer.management.filesystemmanager	INFO
developer.management.fips	INFO
developer.management.fipsmanager	INFO
developer.management.firewall	INFO
developer.management.framework	INFO
developer.management.hardwarestatus	INFO
developer.management.hsmenroll	INFO
developer.management.hsmmoderead	INFO
developer.management.hsmmodesyncmanager	INFO
developer.management.hsmmodewrite	INFO
developer.management.hsmmoduleadd	INFO
developer.management.hsmmoduleremove	INFO
developer.management.hsmmodules	INFO
developer.management.hsmsettingsread	INFO
developer.management.hsmsettingswrite	INFO
developer.management.hsmutility	INFO
developer.management.licenselimits	INFO
developer.management.linuxmanager	INFO
developer.management.linuxmanager.configuration	INFO
developer.management.linuxmanager.etcfacade	INFO
developer.management.linuxmanager.status	INFO
developer.management.loadbalancing	INFO
developer.management.loggingmanager	INFO
developer.management.loggingsnapshotmanager	INFO
developer.management.loginldapmanager	INFO
developer.management.mediastatsnotifier	INFO

Support Log Configuration	
Name	**Level**
developer.management.metricmanager	INFO
developer.management.n2alookup	INFO
developer.management.ntp	INFO
developer.management.optionkeymanager	INFO
developer.management.plugin_loader	INFO
developer.management.provisioning	INFO
developer.management.samlverifier	INFO
developer.management.sch	INFO
developer.management.serviceselectmanager	INFO
developer.management.snmpmanager	INFO
developer.management.sslh	INFO
developer.management.sso	INFO
developer.management.sysctl	INFO
developer.management.systemkey	INFO
developer.management.systemmetricnotifier	INFO
developer.management.systemunit	INFO
developer.management.timemanager	INFO
developer.management.trafficserver	INFO
developer.management.trafficserver.allowlist	INFO
developer.management.trafficserver.cms	INFO
developer.management.trafficserver.oauth	INFO
developer.management.ttylogin	INFO
developer.management.turnloadbalancing	INFO
developer.management.ucqueryrun	INFO
developer.management.ucxnconfig	INFO
developer.management.webcache	INFO
developer.management.webexzoneadd	INFO
developer.management.xcpmanager	INFO
developer.management.xmppdiscovery	INFO
developer.managementconnector	INFO
developer.managementconnector.twisted	INFO
developer.media.configurator	INFO
developer.media.sessionmanager	INFO
developer.media.sessionmanager.mediasession	INFO
developer.media.sessionmanager.turnclient	INFO
developer.mediarouting.core	INFO
developer.mediarouting.manager	INFO
developer.mediarouting.socket	INFO
developer.mediasessionmgr	INFO
developer.mediasessiontestfsm	INFO
developer.modulefactory	INFO
developer.modulefactory.applicationserviceobjectcontroller	INFO
developer.modulefactory.frameworkserviceobjectcontroller	INFO
developer.modulefactory.threadeddispatcher	INFO
developer.networkinterfaceconfig	INFO
developer.ni	INFO
developer.ni.util	INFO
developer.ni.util.web	INFO
developer.ni.util.web.asyncrestclient	INFO
developer.ni.utils	INFO

Support Log Configuration	
Name	**Level**
developer.ni.utils.logging	INFO
developer.ni.utils.logging.plugin	INFO
developer.nomodule	INFO
developer.objectcontroller	INFO
developer.pattern.domain	INFO
developer.pattern_matching	INFO
developer.phonebook	INFO
developer.phpsessionmonitor	INFO
developer.phpsessionmonitor.sessionmonitor	INFO
developer.platform	INFO
developer.platform.amimaster	INFO
developer.platform.ciphermanager	INFO
developer.platform.clusterdatabase	INFO
developer.platform.filesystem	INFO
developer.platform.fips	INFO
developer.platform.network	INFO
developer.platform.platforminfo	INFO
developer.platform.sethostname	INFO
developer.policy	INFO
developer.policymgr.policyservice.connectionchecker	INFO
developer.policymgr.policyservice.connectionmgr.local	INFO
developer.policymgr.policyservice.connectionmgr.remote	INFO
developer.presence	INFO
developer.presence.pua	INFO
developer.provisioning	INFO
developer.qos.configmonitor	INFO
developer.registration.h323	INFO
developer.registration.h323.h323alternateaddresschooser	INFO
developer.registration.h323.regdb	INFO
developer.registration.registrationmgr	INFO
developer.registration.sip	INFO
developer.registration.sip.regdb	INFO
developer.replication	INFO
developer.replication.twisted	INFO
developer.resourcepool	INFO
developer.restapi	INFO
developer.restapi.acme_deploy	INFO
developer.restapi.acme_pendingcert	INFO
developer.restapi.acme_provider	INFO
developer.restapi.acme_settings	INFO
developer.restapi.certs	INFO
developer.restapi.domaincerts	INFO
developer.restapi.hsmenroll	INFO
developer.restapi.hsmmode	INFO
developer.restapi.hsmmodule	INFO
developer.restapi.hsmsettings	INFO
developer.restapi.moebius.db_accessor	INFO
developer.restapi.moebius.transform	INFO
developer.restapi.moebius_app	INFO
developer.restapi.resource	INFO

Support Log Configuration	
Name	**Level**
developer.restapi.twisted	INFO
developer.rshell	INFO
developer.rshellclient	INFO
developer.samba_conf_writer	INFO
developer.samba_helpers	INFO
developer.saml_metadata_exporter.twisted	INFO
developer.sch	INFO
developer.sch.acrrules	INFO
developer.sch.alarmrules	INFO
developer.search	INFO
developer.search.cloudmatching	INFO
developer.search.progress	INFO
developer.serveredge.conn	INFO
developer.servicecontroller	INFO
developer.sip.config	INFO
developer.sip.configmonitor	INFO
developer.sip.dialogmanager	INFO
developer.sip.dispatcher	INFO
developer.sip.dispatcher.clientrequestqueue	INFO
developer.sip.flowtoken	INFO
developer.sip.ice.timer	INFO
developer.sip.identity	INFO
developer.sip.leg	INFO
developer.sip.listener	INFO
developer.sip.mergedrequestsmanager	INFO
developer.sip.msgdisp	INFO
developer.sip.opdb	INFO
developer.sip.partialdecoder	INFO
developer.sip.ping	INFO
developer.sip.procdb	INFO
developer.sip.rendezvousmanager	INFO
developer.sip.services	INFO
developer.sip.transaction	INFO
developer.sip.transactionmanager	INFO
developer.sip.transport	INFO
developer.sip.traversal.binding	INFO
developer.sip.traversal.cfg	INFO
developer.sip.traversal.errs	INFO
developer.sip.traversal.general	INFO
developer.sip.traversal.resp	INFO
developer.sip.traversal.timer	INFO
developer.sipmsg	INFO
developer.sipservice.common.remoteauthzonefactory	INFO
developer.sipservice.proxy.manager	INFO
developer.sipservice.proxy.proxy	INFO
developer.sipservice.proxy.requestrouter	INFO
developer.sipservice.proxy.transport	INFO
developer.sipservice.server	INFO
developer.sipservice.server.digeststatusrequesthandler	INFO
developer.sipservice.server.dsprocessor	INFO

Support Log Configuration	
Name	**Level**
developer.sipservice.server.fsm	INFO
developer.sipservice.server.fsm.impl	INFO
developer.sipservice.server.ntlmstatusresponder	INFO
developer.sipservice.sipservicesync	INFO
developer.sipservice.stats	INFO
developer.sipservice.status	INFO
developer.smart	INFO
developer.smart.soapamlbuilder	INFO
developer.socketpair	INFO
developer.sockhandler	INFO
developer.sshkeychecker.twisted	INFO
developer.sso	INFO
developer.sso.metadata	INFO
developer.sso.metadata.cert	INFO
developer.sso.metadata.cert.creator	INFO
developer.sso.metadata.exporter	INFO
developer.status	INFO
developer.statusmgr	INFO
developer.statusmgr.history	INFO
developer.statusmgr.live	INFO
developer.stderr	INFO
developer.stdout	INFO
developer.stun	INFO
developer.supervisor	INFO
developer.sysadm	INFO
developer.sysadm.mediaportmonitor	INFO
developer.sysadm.serviceselectmonitor	INFO
developer.systemresources	INFO
developer.touchlessdeployment	INFO
developer.touchlessdeployment.twisted	INFO
developer.trafficserver	INFO
developer.trafficserver.allowlist	INFO
developer.transcoder	INFO
developer.transcodermanager	INFO
developer.transcodermanager.launcher	INFO
developer.transcodermanager.twisted	INFO
developer.transcodermanagerclient	INFO
developer.ttlog.monitor	INFO
developer.turn.client	INFO
developer.turn.resourcepool	INFO
developer.turn.resourcepool.mediaprocessorhandler	INFO
developer.turn.resourcepool.stunagent	INFO
developer.upgrade	INFO
developer.userpolicy.sourcealiasrewriter	INFO
developer.utils	INFO
developer.utils.delayedexecutor	INFO
developer.utils.logging	INFO
developer.utils.logging.plugins	INFO
developer.utils.logging.plugins.mediastatssyslog	INFO
developer.utils.periodictimer	INFO

Support Log Configuration	
Name	**Level**
developer.warningfeedbackmanager	INFO
developer.web	INFO
developer.web.app	INFO
developer.web.restclient	INFO
developer.webserv	INFO
developer.winbindservice.fsm.impl	INFO
developer.xcp	INFO
developer.xcp.cm	INFO
developer.xcp.federation	INFO
developer.xcp.jabber	INFO
developer.xmlapi	INFO
developer.xmlapi.administration	INFO
developer.xmlapi.alternates	INFO
developer.xmlapi.apache	INFO
developer.xmlapi.b2buacalls	INFO
developer.xmlapi.b2buaicemetrics	INFO
developer.xmlapi.cdr	INFO
developer.xmlapi.certificationlogging	INFO
developer.xmlapi.ciphers	INFO
developer.xmlapi.cms	INFO
developer.xmlapi.collectdstatus	INFO
developer.xmlapi.commandadapter	INFO
developer.xmlapi.credential	INFO
developer.xmlapi.cucm	INFO
developer.xmlapi.cucmconfig	INFO
developer.xmlapi.edgeauth	INFO
developer.xmlapi.edgeconfigprovisioning	INFO
developer.xmlapi.edgemanagement	INFO
developer.xmlapi.firewall	INFO
developer.xmlapi.getxml	INFO
developer.xmlapi.httpallowlist	INFO
developer.xmlapi.httpproxystats	INFO
developer.xmlapi.httpserver	INFO
developer.xmlapi.json2xml	INFO
developer.xmlapi.log	INFO
developer.xmlapi.mediastats	INFO
developer.xmlapi.microsoft_b2bua	INFO
developer.xmlapi.networkinterface	INFO
developer.xmlapi.optionkeys	INFO
developer.xmlapi.plugins	INFO
developer.xmlapi.portforwarding	INFO
developer.xmlapi.protocolqos	INFO
developer.xmlapi.putxml	INFO
developer.xmlapi.sipdomain	INFO
developer.xmlapi.sso	INFO
developer.xmlapi.ucnode	INFO
developer.xmlapi.ucxnconfig	INFO
developer.xmlapi.uds	INFO
developer.xmlapi.xmppdiscovery	INFO
developer.xmlapi.xmpphistory	INFO

Support Log Configuration	
Name	**Level**
developer.xmlapi.xmppstats	INFO
developer.xmlappl	INFO
developer.zone.activepeerchooser	INFO
developer.zone.dnszone	INFO
developer.zone.enumzone	INFO
developer.zone.neighbourzone	INFO
developer.zone.traversalclientzone	INFO
developer.zone.traversalserverzone	INFO
developer.zone.zonemgr	INFO