Cisco TelePresence Video Communication Server

Command Reference

D14754.01

January 2010

Software version: X6

Contents

Introduction

This Command Reference document provides supplementary information regarding the administration of the Cisco TelePresence Video Communication Server (Cisco VCS). It includes:

- details of the commands available through the Cisco VCS's command line interface (CLI)
- a description of the parameters included in requests from the Cisco VCS to external policy services

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.

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.

CLI command types

CLI commands are divided into the following groups:

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

Note that:

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

xConfiguration command reference

The **xConfiguration** group of commands are used to set and change individual items of configuration. Each command is made up of a main element followed by one or more sub-elements.

The following section lists all the currently available **xConfiguration** commands.

To set a particular item of configuration, type the command as shown. The valid values for each command are indicated in the angle brackets following each command, using the following notation:

Format	Meaning
<0..63>	Indicates an integer value is required. The numbers indicate the minimum and maximum value. In this example the value must be in the range 0 to 63.
<S: 7,15>	An **S** indicates a string value, to be enclosed in quotation marks, is required. The numbers indicate the minimum and maximum number of characters for the string. In this example the string must be between 7 and 15 characters long.
<Off/Direct/Indirect>	Lists the set of valid values for the command. Do not enclose the value in quotation marks
[1..50]	Square brackets indicate that you can configure more than one of this particular item. Each item is assigned an index within the range shown. For example **IP Route [1..50] Address <S: 0,39>** means that up to 50 IP routes can be specified with each route requiring an address of up to 39 characters in length.

To obtain information about existing configuration, type:

- **xConfiguration** to return all current configuration settings
- **xConfiguration <element>** to return all current configuration for that particular element and all its sub-elements
- **xConfiguration <element> <subelement>**to return all current configuration for that group of sub-elements

To obtain information about using each of the **xConfiguration** commands, type:

- **xConfiguration ?** to return a list of all elements available under the **xConfiguration**command
- **xConfiguration ??** to return a list of all elements available under the **xConfiguration**command, along with the valuespace, description and default values for each element
- **xConfiguration <element> ?** to return all available sub-elements and their valuespace, description and default values
- **xConfiguration <element> <sub-element> ?** to return all available sub-elements and their valuespace, description and default values

xConfiguration commands

All of the available **xConfiguration** commands are listed in the table below:

Administration HTTP Mode: <On/Off>

Determines whether HTTP calls will be redirected to the HTTPS port.

On: calls will be redirected to HTTPS.

Off: no HTTP access will be available.

Note: you must restart the system for any changes to take effect.

Default: On

Example: **xConfiguration Administration HTTP Mode: On**

Administration HTTPS Mode: <On/Off>

Determines whether the VCS can be accessed via the web interface. This must be On to enable both web interface and TMS access.

Note: you must restart the system for any changes to take effect.

Default: On

Example: **xConfiguration Administration HTTPS Mode: On**

Administration HTTPS RequireClientCertificate: <On/Off>

Determines whether the VCS requires a valid client certificate from your web browser before setting up an HTTPS session. Note: this does not affect client verification of the VCS's server certificate.

Default: Off

Example: **xConfiguration Administration HTTPS RequireClientCertificate: On**

Administration LCDPanel Mode: <On/Off>

Controls whether the LCD panel on the front of the VCS identifies the system.

On: the system name and first active IP address are shown.

Off: the LCD panel reveals no identifying information about the system.

Default: On

Example: **xConfiguration Administration LCDPanel Mode: On**

Administration SSH Mode: <On/Off>

Determines whether the VCS can be accessed via SSH and SCP.

Note: you must restart the system for any changes to take effect.

Default: On

Example: **xConfiguration Administration SSH Mode: On**

Administration Telnet Mode: <On/Off>

Determines whether the VCS can be accessed via Telnet.

Note: you must restart the system for any changes to take effect.

Default: Off

Example: **xConfiguration Administration Telnet Mode: Off**

Administration TimeOut: <0..10000>

Sets the number of minutes that an administration session (HTTPS, Telnet or SSH) may be inactive before the session is timed out. A value of 0 turns session time outs off.

Default: 0

Example: **xConfiguration Administration TimeOut: 0**

Alternates Cluster Name: <S: 0,128>

The fully qualified domain name used in SRV records that address this VCS cluster, for example "cluster1.example.com". The name can only contain letters, digits, hyphens and underscores.

Warning: if you change the cluster name after any user accounts have been configured on this VCS, you may need to reconfigure your user accounts to use the new cluster name. Refer to the Clustering and peers section of the VCS Administrator Guide for more information.

Example: **`xConfiguration Alternates Cluster Name: "Regional"`**

Alternates ConfigurationMaster: <1..6>

Specifies which peer in this cluster is the master, from which configuration will be replicated to all other peers. A cluster consists of up to 6 peers, including the local VCS.

Example: **`xConfiguration Alternates ConfigurationMaster: 1`**

Alternates Peer [1..6] Address: <S: 0, 128>

Specifies the IP address of one of the peers in the cluster to which this VCS belongs. A cluster consists of up to 6 peers, including the local VCS.

Note: this must be a valid IPv4 or IPv6 address.

Example: **`xConfiguration Alternates 1 Peer Address: "10.13.0.2"`**

Applications ConferenceFactory Alias: <S:0,60>

The alias that will be dialed by the endpoints when the Multiway feature is activated. This must be pre-configured on all endpoints that may be used to initiate the Multiway feature.

Example: **`xConfiguration Applications ConferenceFactory Alias: "multiway@example.com"`**

Applications ConferenceFactory Mode: <On/Off>

The Mode option allows you to enable or disable the Conference Factory application.

Default: Off

Example: **`xConfiguration Applications ConferenceFactory Mode: Off`**

Applications ConferenceFactory Range End: <1..65535>

The last number of the range that replaces %% in the template used to generate a conference alias.

Default: 65535

Example: **`xConfiguration Applications ConferenceFactory Range End: 30000`**

Applications ConferenceFactory Range Start: <1..65535>

The first number of the range that replaces %% in the template used to generate a conference alias.

Default: 65535

Example: **`xConfiguration Applications ConferenceFactory Range Start: 10000`**

Applications ConferenceFactory Template: <S:0,60>

The alias that the VCS will tell the endpoint to dial in order to create a Multiway conference on the MCU.

Note: this alias must route to the MCU as a fully-qualified SIP alias

Example: **`Applications ConferenceFactory Template: "563%%@example.com"`**

Applications External Status [1..10] Filename: <S:0,255>

XML file containing status that is to be attached for an external application.

Example: **`xConfiguration Applications External Status 1 Filename: "foo.xml"`**

Applications External Status [1..10] Name: <S:0,64>

Descriptive name for the external application whose status is being referenced.

Example: **xConfiguration Applications External Status 1 Name: "foo"**

Applications OCS Relay Mode: <On/Off>

Enables or disables OCS relay support.

Default: Off

Example: **xConfiguration Applications OCS Relay Mode: Off**

Applications OCS Relay OCS Domain: <S:0,128>

The SIP domain in use on the Microsoft Office Communications Server. This must be selected from one of the SIP domains already configured on the VCS, and must be the same domain used by all FindMe names.

Example: **xConfiguration Applications OCS Relay OCS Domain: "example.com"**

Applications OCS Relay OCS Routing Prefix: <S:0,128>

Prefix applied to requests routed through the VCS proxy, from the OCS Relay. This is then used to route the requests onto to the appropriate Microsoft Office Communications Server (via Neighbor zone matches).

Default: ocs

Example: **xConfiguration Applications OCS Relay OCS Routing Prefix: "ocs"**

Applications Presence Server Mode: <On/Off>

Enables and disables the SIMPLE Presence Server. Note: SIP mode must also be enabled for the Presence Server to function.

Default: Off

Example: **xConfiguration Applications Presence Server Mode: On**

Applications Presence Server Publication ExpireDelta: <30..7200>

Specifies the maximum time (in seconds) within which a publisher must refresh its publication.

Default: 1800

Example: **xConfiguration Applications Presence Server Publication ExpireDelta: 1800**

Applications Presence Server Subscription ExpireDelta: <30..7200>

Specifies the maximum time (in seconds) within which a subscriber must refresh its subscription.

Default: 3600

Example: **xConfiguration Applications Presence Server Subscription ExpireDelta: 3600**

Applications Presence User Agent ExpireDelta: <1..65534>

Specifies the lifetime value (in seconds) the Presence User Agent will advertise in the PUBLISH messages it sends to the Presence Server. The Presence User Agent will refresh its PUBLISH messages at 75% of this value (to keep them active). The Presence Server may reduce this value in its responses.

Default: 3600

Example: **xConfiguration Applications Presence User Agent ExpireDelta: 3600**

Applications Presence User Agent Mode: <On/Off>

Enables and disables the SIMPLE Presence User Agent (PUA). The PUA provides presence information on behalf of registered endpoints. SIP mode must also be enabled for the PUA to function.

Default: Off

Example: **xConfiguration Applications Presence User Agent Mode: Off**

Applications Presence User Agent RetryDelta: <1..65534>

Specifies the time (in seconds) after which the Presence User Agent will attempt to resend a PUBLISH to the Presence Server. This will occur if the original attempt failed due to resource issues or other transitory errors.

Default: 1800

Example: **xConfiguration Applications Presence User Agent RetryDelta: 1800**

Authentication ADS ADDomain: <S: 0,255>

The Kerberos realm used when the VCS joins the AD domain. Note: this field is case sensitive.

Example: **xConfiguration Authentication ADS ADDomain:**

Authentication ADS Clockskew: <1..65535>

Maximum allowed clockskew between the VCS and the KDC before the Kerberos message is assumed to be invalid (in seconds).

Default: 300

Example: **xConfiguration Authentication ADS Clockskew: 300**

Authentication ADS DC [1..5] Address: <S: 0,39>

The address of a domain controller that can be used when the VCS joins the AD domain. Not specifying a specific AD will result the use of DNS SRV queries to find an AD.

Example: **xConfiguration Authentication ADS DC 1 Address: "192.168.0.0"**

Authentication ADS Encryption: <Off/TLS>

Sets the encryption to use for the connection to the ADS server.

Off: no encryption is used.

TLS: TLS encryption is used.

Default: TLS

Example: **xConfiguration Authentication ADS Encryption: TLS**

Authentication ADS KDC [1..5] Address: <S: 0,39>

The address of a Kerberos Distribution Center (KDC) to be used when connected to the AD domain. Not specifying a specific KDC will result in the use of DNS SRV queries to find a KDC.

Example: **xConfiguration Authentication ADS KDC 1 Address: "192.168.0.0"**

Authentication ADS KDC [1..5] Port: <1..65534>

Specifies the port of a KDC that can be used when the VCS joins the AD domain.

Default: 88

Example: **xConfiguration Authentication ADS KDC 1 Port: 88**

Authentication ADS Mode: <On/Off>

Indicates if the VCS should attempt to form a relationship with the AD.

Default: Off

Example: **xConfiguration Authentication ADS Mode: On**

Authentication ADS SPNEGO: <Enabled/Disabled>

Indicates if SPNEGO (Simple and Protected GSSAPI Negotiation Mechanism) is used when the client (the VCS) authenticates with the server (the AD domain controller).

Default: Enabled

Example: **xConfiguration Authentication ADS SPNEGO: Enabled**

Authentication ADS SecureChannel: <Auto/Enabled/Disabled>

Indicates if data transmitted from the VCS to an AD domain controller is sent over a secure channel.

Default: Auto

Example: **xConfiguration Authentication ADS SecureChannel: Auto**

Authentication ADS Workgroup: <S: 0,15>

The workgroup used when the VCS joins the AD domain.

Example: **xConfiguration Authentication ADS Workgroup:**

Authentication Credential [1..2500] Name: <S: 0, 128>

Defines the name for this entry in the local authentication database.

Example: **xConfiguration Authentication Credential 1 Name: "john smith"**

Authentication Credential [1..2500] Password: <S: 0, 215>

Defines the password for this entry in the local authentication database. The maximum plaintext length is 128 characters, which will then be encrypted.

Example: **xConfiguration Authentication Credential 1 Password: "password123"**

Authentication Database: <LocalDatabase/LDAPDatabase>

Selects between a local authentication database and a remote LDAP repository for the storage of password information for authentication.

Default: LocalDatabase

Example: **xConfiguration Authentication Database: LocalDatabase**

Authentication LDAP AliasOrigin: <LDAP/Endpoint/Combined>

Determines which aliases (i.e. from the LDAP repository or the endpoint) should be used to register the endpoint.

Combined: the endpoint will be registered both with the aliases which it has presented and with those configured in the LDAP repository.

Default: LDAP

Example: **xConfiguration Authentication LDAP AliasOrigin: LDAP**

Authentication LDAP BaseDN: <S: 0, 255>

Specifies the Distinguished Name to use when connecting to an LDAP server.

Example: xConfiguration Authentication LDAP BaseDN: "dc=example,dc=company,dc=com"

Authentication Password: <S: 0, 215>

The password used by the VCS when authenticating with another system. The maximum plaintext length is 128 characters, which is then encrypted. Note: this does not apply to traversal client zones.

Example: **xConfiguration Authentication Password: "password123"**

Authentication UserName: <S: 0, 128>

The username used by the VCS when authenticating with another system. Note: this does not apply to traversal client zones.

Example: **xConfiguration Authentication UserName: "VCS123"**

Bandwidth Default: <64..65535>

Sets the bandwidth (in kbps) to be used on calls managed by the VCS in cases where no bandwidth has been specified by the endpoint.

Default: 384

Example: **xConfiguration Bandwidth Default: 384**

Bandwidth Downspeed PerCall Mode: <On/Off>

Determines whether or not the VCS will attempt to downspeed a call if there is insufficient per-call bandwidth available to fulfill the request.

On: the VCS will attempt to place the call at a lower bandwidth.

Off: the call will be rejected.

Default: On

Example: **xConfiguration Bandwidth Downspeed PerCall Mode: On**

Bandwidth Downspeed Total Mode: <On/Off>

Determines whether or not the VCS will attempt to downspeed a call if there is insufficient total bandwidth available to fulfill the request.

On: the VCS will attempt to place the call at a lower bandwidth.

Off: the call will be rejected.

Default: On

Example: **xConfiguration Bandwidth Downspeed Total Mode: On**

Bandwidth Link [1..3000] Name: <S: 1, 50>

Assigns a name to this link.

Example: **xConfiguration Bandwidth Link 1 Name: "HQ to BranchOffice"**

Bandwidth Link [1..3000] Node1 Name: <S: 0, 50>

Specifies the first zone or subzone to which this link will be applied.

Example: **xConfiguration Bandwidth Link 1 Node1 Name: "HQ"**

Bandwidth Link [1..3000] Node2 Name: <S: 0, 50>

Specifies the second zone or subzone to which this link will be applied.

Example: **xConfiguration Bandwidth Link 1 Node2 Name: "BranchOffice"**

Bandwidth Link [1..3000] Pipe1 Name: <S: 0, 50>

Specifies the first pipe to be associated with this link.

Example: **xConfiguration Bandwidth Link 1 Pipe1 Name: "512Kb ASDL"**

Bandwidth Link [1..3000] Pipe2 Name: <S: 0, 50>

Specifies the second pipe to be associated with this link.

Example: **xConfiguration Bandwidth Link 1 Pipe2 Name: "2Gb Broadband"**

Bandwidth Pipe [1..1000] Bandwidth PerCall Limit: <1..100000000>

If this pipe has limited per-call bandwidth, sets the maximum amount of bandwidth (in kbps) available for any one call.

Default: 1920

Example: **xConfiguration Bandwidth Pipe 1 Bandwidth PerCall Limit: 256**

Bandwidth Pipe [1..1000] Bandwidth PerCall Mode: <Limited/Unlimited/NoBandwidth>

Determines whether or not this pipe is limiting the bandwidth of individual calls.

NoBandwidth: no bandwidth available. No calls can be made on this pipe.

Default: Unlimited

Example: **xConfiguration Bandwidth Pipe 1 Bandwidth PerCall Mode: Limited**

Bandwidth Pipe [1..1000] Bandwidth Total Limit: <1..100000000>

If this pipe has limited bandwidth, sets the maximum bandwidth (in kbps) available at any one time on the pipe.

Default: 500000

Example: **xConfiguration Bandwidth Pipe 1 Bandwidth Total Limit: 1024**

Bandwidth Pipe [1..1000] Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth>

Determines whether or not this pipe is enforcing total bandwidth restrictions.

NoBandwidth: no bandwidth available. No calls can be made on this pipe.

Default: Unlimited

Example: **xConfiguration Bandwidth Pipe 1 Bandwidth Total Mode: Limited**

Bandwidth Pipe [1..1000] Name: <S: 1, 50>

Assigns a name to this pipe.

Example: **xConfiguration Bandwidth Pipe 1 Name: "512Kb ASDL"**

Call Loop Detection Mode: <On/Off>

Specifies whether the VCS will check for call loops.

Default: On

Example: **xConfiguration Call Loop Detection Mode: On**

Call Routed Mode: <Always/Optimal>

Specifies whether the VCS routes the signaling for calls.

Always: the VCS will always route the call signaling.

Optimal: if possible, the VCS will remove itself from the call signaling path, which may mean the call does not consume a call license.

Default: Always

Example: **xConfiguration Call Routed Mode: Always**

Call Services CallsToUnknownIPAddresses: <Off/Direct/Indirect>

Determines the way in which the VCS will attempt to call systems which are not registered with it or one of its neighbors.

Direct: allows an endpoint to make a call to an unknown IP address without the VCS querying any neighbors. The call setup would occur just as it would if the far end were registered directly to the local system.

Indirect: upon receiving a call to an unknown IP address, the VCS will query its neighbors for the remote address and if permitted will route the call through the neighbor.

Off: endpoints registered directly to the VCS may only call an IP address of a system also registered directly to that VCS.

Default: Indirect

Example: `xConfiguration Call Services CallsToUnknownIPAddresses: Indirect`

Call Services Fallback Alias: <S: 0, 60>

Specifies the alias to which incoming calls are placed for calls where the IP address or domain name of the VCS has been given but no callee alias has been specified.

Example: `xConfiguration Call Services Fallback Alias: "reception@example.com"`

Certification AdvancedAccountSecurity Mode: <On/Off>

Enables or disables advanced account security. Note: you must restart the system for any changes to take effect.

Default: Off

Example: `xConfiguration Certification AdvancedAccountSecurity Mode: On`

Core Dump Mode: <On/Off>

Controls whether application core dumps are enabled. Note: you must restart the system for any changes to take effect.

Default: Off

Example: `xConfiguration Core Dump Mode: Off`

Error Reports Mode: <On/Off>

Determines whether the VCS will automatically send details of application failures to a specified web service.

Default: Off

Example: `xConfiguration Error Reports Mode: Off`

Error Reports URL: <S: 0, 128>

The URL of the web service to which error reports are sent.

Default: http://vcser.tandberg.com/submitapplicationerror/

Example: `xConfiguration Error Reports URL: "http://vcser.tandberg.com/submitapplicationerror/"`

Ethernet [1..2] IP V4 Address: <S: 7,15>

Specifies the IPv4 address of the specified LAN port. Note: you must restart the system for any changes to take effect.

Example: `xConfiguration Ethernet 1 IP V4 Address: "192.168.10.10"`

Ethernet [1..2] IP V4 StaticNAT Address: <S:7,15>

If the VCS is operating in static NAT mode, this specifies the external public IPv4 address of that static NAT. Note: you must restart the system for any changes to take effect.

Example: `xConfiguration Ethernet 1 IP V4 StaticNAT Address: "64.22.64.85"`

Ethernet [1..2] IP V4 StaticNAT Mode: <On/Off>

Specifies whether the VCS is located behind a static NAT. Note: You must restart the system for any changes to take effect.

Default: Off

Example: `xConfiguration Ethernet 1 IP V4 StaticNAT Mode: On`

Ethernet [1..2] IP V4 SubnetMask: <S: 7,15>

Specifies the IPv4 subnet mask of the specified LAN port. Note: you must restart the system for any changes to take effect.

Example: `xConfiguration Ethernet 1 IP V4 SubnetMask: "255.255.255.0"`

Ethernet [1..2] IP V6 Address: <S: 0, 39>

Specifies the IPv6 address of the specified LAN port. Note: you must restart the system for any changes to take effect.

Example: `xConfiguration Ethernet 1 IP V6 Address: "2001:db8::1428:57ab"`

Ethernet [1..2] Speed: <Auto/10half/10full/100half/100full/1000full

Sets the speed of the Ethernet link from the specified LAN port. Use Auto to automatically configure the speed. Note: you must restart the system for any changes to take effect.

Default: Auto

Example: `xConfiguration Ethernet 1 Speed: Auto`

ExternalManager Address: <S: 0, 128>

Sets the IP address or Fully Qualified Domain Name (FQDN) of the external manager.

Example: `xConfiguration ExternalManager Address: "192.168.0.0"`

ExternalManager Path: <S: 0, 255>

Sets the URL of the external manager.

Default: tms/public/external/management/SystemManagementService.asmx

Example: `xConfiguration ExternalManager Path: "tms/public/external/management/SystemManagementService.asmx"`

ExternalManager Protocol: <HTTP/HTTPS>

The protocol used to connect to the external manager.

Default: HTTP

Example: `xConfiguration ExternalManager Protocol: HTTP`

ExternalManager Server Certificate Verification Mode: <On/Off>

Controls whether the certificate presented by the external manager is verified.

Default: On

Example: `xConfiguration ExternalManager Server Certificate Verification Mode: On`

H323 Gatekeeper AutoDiscovery Mode: <On/Off>

Determines whether or not the VCS responds to gatekeeper discovery requests from endpoints.

Default: On

Example: `xConfiguration H323 Gatekeeper AutoDiscovery Mode: On`

H323 Gatekeeper CallSignaling PortRange End: <1024..65534>

Specifies the upper port in the range to be used by calls once they are established.

Default: 19999

Example: `xConfiguration H323 Gatekeeper CallSignaling PortRange End: 19999`

H323 Gatekeeper CallSignaling PortRange Start: <1024..65534>

Specifies the lower port in the range to be used by calls once they are established.

Default: 15000

Example: `xConfiguration H323 Gatekeeper CallSignaling PortRange Start: 15000`

H323 Gatekeeper CallSignaling TCP Port: <1024..65534>

Specifies the port that listens for H.323 call signaling.

Default: 1720

Example: `xConfiguration H323 Gatekeeper CallSignaling TCP Port: 1720`

H323 Gatekeeper CallTimeToLive: <60..65534>

Specifies the interval (in seconds) at which the VCS polls the endpoints in a call to verify that they are still in the call.

Default: 120

Example: `xConfiguration H323 Gatekeeper CallTimeToLive: 120`

H323 Gatekeeper Registration ConflictMode: <Reject/Overwrite>

Determines how the system will behave if an endpoint attempts to register an alias currently registered from another IP address.

Reject: denies the registration.

Overwrite: deletes the original registration and replaces it with the new registration.

Default: Reject

Example: `xConfiguration H323 Gatekeeper Registration ConflictMode: Reject`

H323 Gatekeeper Registration UDP Port: <1024..65534>

Specifies the port to be used for H.323 UDP registrations.

Default: 1719

Example: `xConfiguration H323 Gatekeeper Registration UDP Port: 1719`

H323 Gatekeeper TimeToLive: <60..65534>

Specifies the interval (in seconds) at which an H.323 endpoint must re-register with the VCS in order to confirm that it is still functioning.

Default: 1800

Example: `xConfiguration H323 Gatekeeper TimeToLive: 1800`

H323 Gateway CallerId: <IncludePrefix/ExcludePrefix>

Specifies whether the prefix of the ISDN gateway is inserted into the caller's E.164 number presented on the destination endpoint. Including the prefix allows the recipient to directly return the call.

IncludePrefix: inserts the ISDN gateway's prefix into the source E.164 number.

ExcludePrefix: only displays the source E.164 number.

Default: ExcludePrefix

Example: **`xConfiguration H323 Gateway CallerId: ExcludePrefix`**

H323 Mode: <On/Off>

Determines whether or not the VCS will provide H.323 gatekeeper functionality.

Default: On

Example: **`xConfiguration H323 Mode: On`**

Interworking Encryption Mode: <Auto/Off>

Determines whether or not the VCS will allow encrypted calls between SIP and H.323 endpoints.

Off: interworked calls will never be encrypted.

Auto: interworked calls will be encrypted if the endpoints request it.

Default: Auto

Example: **`xConfiguration Interworking Encryption Mode: Auto`**

Interworking Encryption Replay Protection Mode: <On/Off>

Controls whether the VCS will perform replay protection for incoming SRTP packets when interworking a call.

On: replayed SRTP packets will be dropped by the VCS.

Off: the VCS will not check for replayed SRTP packets.

Default: Off

Example: **`xConfiguration Interworking Encryption Replay Protection Mode: Off`**

Interworking Mode: <On/Off/RegisteredOnly>

Determines whether or not the VCS will act as a gateway between SIP and H.323 calls.

Off: the VCS will not act as a SIP-H.323 gateway.

On: the VCS will act as SIP-H.323 gateway regardless of whether the endpoints are locally registered.

RegisteredOnly: the VCS will act as a SIP-H.323 gateway but only if at least one of the endpoints is locally registered.

Default: RegisteredOnly

Example: **`xConfiguration Interworking Mode: RegisteredOnly`**

IP DNS Domain Name: <S: 0, 128>

The name to be appended to an unqualified host name before querying the DNS server.

Used only when attempting to resolve unqualified domain names for NTP, LDAP, external manager and remote syslog servers.

Example: **`xConfiguration IP DNS Domain Name: "example.com"`**

IP DNS Hostname : <S: 0, 63>

Defines the DNS host name that this system is known by. Note that this is not the fully-qualified domain name, just the host label portion.

The name can only contain letters, digits, hyphens and underscores. The first character must be a letter and the last character must be a letter or a digit.

Example: `xConfiguration IP DNS Hostname: "localvcs"`

IP DNS Server [1..5] Address: <S: 0, 39>

Sets the IP address of up to 5 DNS servers to be used when resolving domain names.

Example: `xConfiguration IP DNS Server 1 Address: "192.168.12.0"`

IP Ephemeral PortRange End: <1024..65534>

Specifies the highest port in the range to be used for ephemeral outbound connections not otherwise constrained by VCS call processing.

Default: 49999

Example: `xConfiguration IP Ephemeral PortRange End: 49999`

IP Ephemeral PortRange Start: <1024..65534>

Specifies the lowest port in the range to be used for ephemeral outbound connections not otherwise constrained by VCS call processing.

Default: 40000

Example: `xConfiguration IP Ephemeral PortRange Start: 40000`

IP External Interface: <LAN1/LAN2>

Defines which LAN interface is externally facing.

Default: LAN1

Example: `xConfiguration IP External Interface: LAN1`

IP Gateway: <S: 7,15>

Specifies the IPv4 gateway of the VCS. Note: you must restart the system for any changes to take effect.

Default: 127.0.0.1

Example: `xConfiguration IP Gateway: "192.168.127.0"`

IP QoS Mode: <None/DiffServ>

Specifies the type of QoS (Quality of Service) tags to apply to all signaling and media packets.

None: no specific QoS tagging is applied.

DiffServ: puts the specified Tag value in the TOS (Type Of Service) field of the IPv4 header or TC (Traffic Class) field of the IPv6 header.

Note: you must restart the system for any changes to take effect.

Default: None

Example: `xConfiguration IP QoS Mode: DiffServ`

IP QoS Value: <0..63>

The value to be stamped onto all signaling and media traffic routed through the VCS. Note: you must restart the system for any changes to take effect.

Example: `xConfiguration IP QoS Value: 16`

IP Route [1..50] Address: <S: 0, 39>

Specifies an IP address used in conjunction with the Prefix Length to determine the network to which this route applies.

Example: `xConfiguration IP Route 1 Address: "128.168.0.0"`

IP Route [1..50] Gateway: <S: 0, 39>

Specifies the IP address of the Gateway for this route.

Example: `xConfiguration IP Route 1 Gateway: "192.168.0.0"`

IP Route [1..50] Interface: <Auto/LAN1/LAN2>

Specifies the LAN interface to use for this route. Auto: The VCS will select the most appropriate interface to use.

Default: Auto

Example: `xConfiguration IP Route 1 Interface: Auto`

IP Route [1..50] PrefixLength: <0..128>

Specifies the number of bits of the IP address which must match when determining the network to which this route applies.

Default: 32

Example: `xConfiguration IP Route 1 PrefixLength: 16`

IP V6 Gateway: <S: 0, 39>

Specifies the IPv6 gateway of the VCS. Note: you must restart the system for any changes to take effect.

Example: `xConfiguration IP V6 Gateway: "3dda:80bb:6::9:144"`

IPProtocol: <Both/IPv4/IPv6>

Selects whether the VCS is operating in IPv4, IPv6 or dual stack mode. Note: you must restart the system for any changes to take effect.

Default: IPv4

Example: `xConfiguration IPProtocol: IPv4`

LDAP Encryption: <Off/TLS>

Sets the encryption to use for the connection to the LDAP server.

Off: no encryption is used.

TLS: TLS encryption is used.

Default: Off

Example: `xConfiguration LDAP Encryption: Off`

LDAP Password: <S: 0, 122>

Sets the password to use when binding to the LDAP server. The maximum plaintext length is 60 characters, which is then encrypted.

Example: `xConfiguration LDAP Password: "password123"`

LDAP Server Address: <S: 0, 128>

Sets the IP address or Fully Qualified Domain Name (FQDN) of the LDAP server to use when making LDAP queries.

Example: `xConfiguration LDAP Server Address: "ldap.server.example.com"`

LDAP Server Port: <1..65534>

Sets the IP port of the LDAP server to use when making LDAP queries. Typically, non-secure connections use 389 and secure connections use 636.

Default: 389

Example: `xConfiguration LDAP Server Port: 389`

LDAP UserDN: <S: 0, 255>

Sets the user distinguished name to use when binding to the LDAP server.

Example: `xConfiguration LDAP UserDN: "user123"`

Log Level: <1..4>

Controls the granularity of Event Logging. 1 is the least verbose, 4 the most.

Note: this setting is not retrospective; it will determine which events are written to the Event Log from now onwards.

Default: 1

Example: `xConfiguration Log Level: 1`

Log Server Address: <S: 0, 128>

A comma-separated list of IP addresses or Fully Qualified Domain Names (FQDNs) of the remote syslog servers to where the Event Log is written. These servers must support the BSD syslog protocol. They cannot be another VCS.

Example: `xConfiguration Log Server Address: "syslog.server.example.com"`

Login Administrator Groups Group [1..30] Access: <None/ReadOnly/ReadWrite/Auditor>

Defines the access level for members of the specified administrator group.

None: no access allowed.

ReadOnly: configuration can only be viewed.

ReadWrite: configuration can be viewed and changed.

Auditor: allows access to the Event Log, Configuration Log and the Overview page only.

Default: ReadWrite

Example: `xConfiguration Login Administrator Groups Group 1 Access: ReadWrite`

Login Administrator Groups Group [1..30] Name: <S: 0,128>

Defines the name of an administrator group that determines which access rights members of the group have after they have been successfully authenticated to use the VCS.

Example: `xConfiguration Login Administrator Groups Group 1 Name: "VCS_Admin"`

Login Administrator Source: <Local/Remote>

Defines where administrator login credentials are authenticated before access is allowed to the VCS.

Remote: credentials are verified against an external credentials directory, for example Windows Active Directory.

Local: credentials are verified against a local database stored on the VCS.

Default: Local

Example: `xConfiguration Login Administrator Source: Local`

Login Remote LDAP BaseDN Accounts: <S: 0,255>

Sets the Distinguished Name to use as the base when searching for administrator and user accounts.

Example: **xConfiguration Login Remote LDAP BaseDN Accounts: "ou=useraccounts,dc=corporation,dc=int"**

Login Remote LDAP BaseDN Groups: <S: 0,255>

Sets the Distinguished Name to use as the base when searching for administrator and user groups.

Example: **xConfiguration Login Remote LDAP BaseDN Groups: "ou=groups,dc=corporation,dc=int"**

Login Remote LDAP CRLCheck: <None/Peer/All>

Specifies whether certificate revocation lists (CRLs) are checked when forming a TLS connection with the LDAP server. CRL data is uploaded to the VCS via the trusted CA certificate PEM file.

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.

Default: None.

Example: **xConfiguration Login Remote LDAP CRLCheck: Peer**

Login Remote LDAP DirectoryType: <ActiveDirectory>

Defines the type of LDAP directory that is being accessed.

ActiveDirectory: directory is Windows Active Directory.

Default: ActiveDirectory

Example: **xConfiguration Login Remote LDAP DirectoryType: ActiveDirectory**

Login Remote LDAP Encryption: <Off/TLS>

Sets the encryption to use for the connection to the LDAP server.

Off: no encryption is used.

TLS: TLS encryption is used.

Default: Off

Example: **xConfiguration Login Remote LDAP Encryption: Off**

Login Remote LDAP SASL: <None/DIGEST-MD5>

Sets 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.

Default: DIGEST-MD5

Example: **xConfiguration Login Remote LDAP SASL: DIGEST-MD5**

Login Remote LDAP Server Address: <S: 0,128>

Sets the IP address or Fully Qualified Domain Name (FQDN) of the LDAP server to use when making LDAP queries.

Example: **xConfiguration Login Remote LDAP Server Address: "server.example.com"**

Login Remote LDAP Server FQDNResolution: <AddressRecord/SRVRecord>

Sets how the LDAP server address is resolved if specified as an FQDN.

AddressRecord: DNS A or AAAA record lookup.

SRVRecord: DNS SRV record lookup.

Default: AddressRecord

Example: **xConfiguration Login Remote LDAP Server FQDNResolution: AddressRecord**

Login Remote LDAP Server Port: <1..65534>

Sets the IP port of the LDAP server to use when making LDAP queries. Typically, non-secure connections use 389 and secure connections use 636.

Default: 389

Example: **xConfiguration Login Remote LDAP Server Port: 389**

Login Remote LDAP VCS BindDN: <S: 0,255>

Sets the user distinguished name to use when binding to the LDAP server.

Example: **xConfiguration Login Remote LDAP VCS BindDN: "VCSmanager"**

Login Remote LDAP VCS BindPassword: <S: 0,122>

Sets the password to use when binding to the LDAP server. The maximum plaintext length is 60 characters, which is then encrypted.

Example: **xConfiguration Login Remote LDAP VCS BindPassword: "password123"**

Login Remote LDAP VCS BindUsername: <S: 0,255>

Sets the username to use when binding to the LDAP server. Only applies if using SASL.

Example: **xConfiguration Login Remote LDAP VCS BindUsername: "VCSmanager"**

Login Remote Protocol: <LDAP>

The protocol used to connect to the external directory.

Default: LDAP

Example: **xConfiguration Login Remote Protocol: LDAP**

Login User Groups Group [1..15] Access: <None/ReadWrite>

Defines the access level for members of the specified user group.

None: no access allowed.

ReadWrite: configuration can be viewed and changed.

Default: ReadWrite

Example: **xConfiguration Login User Groups Group 1 Access: ReadWrite**

Login User Groups Group [1..15] Name: <S: 0,128>

Defines the name of a user group that determines which access rights members of the group have after they have been successfully authenticated to use the VCS.

Example: **xConfiguration Login User Groups Group 1 Name: "FindMeAccounts"**

Login User Source: <Local/Remote>

Defines where user login credentials are authenticated before access is allowed to the VCS.

Remote: credentials are verified against an external credentials directory, for example Windows Active Directory.

Local: credentials are verified against a local database stored on the VCS.

Default: Local

Example: **xConfiguration Login User Source: Local**

NTP Address: <S: 0, 128>

Sets the IP address or Fully Qualified Domain Name (FQDN) of the NTP server to be used when synchronizing system time.

Example: **xConfiguration NTP Address: "ntp.server.example.com"**

Option [1..64] Key: <S: 0, 90>

Specifies the option key of your software option. These are added to the VCS in order to add extra functionality, such as increasing the VCS's capacity. Contact your TANDBERG representative for further information.

Example: **xConfiguration Option 1 Key: "1X4757T5-1-60BAD5CD"**

Policy AdministratorPolicy Mode: <Off/LocalCPL/LocalService/PolicyService>

Enables and disables use of Call Policy.

Off: Disables call policy.

LocalCPL: uses policy from an uploaded CPL file.

LocalService: uses group policy information and a local file.

PolicyService: uses an external policy server.

Default: Off

Example: **xConfiguration Policy AdministratorPolicy Mode: Off**

Policy AdministratorPolicy Service DefaultCPL: <S: 0,255>

The CPL used by the VCS when the remote service is unavailable.

Default: <reject status='403' reason='Service Unavailable'/>

Example: **xConfiguration Policy AdministratorPolicy Service DefaultCPL: "<reject status='403' reason='Service Unavailable'/>"**

Policy AdministratorPolicy Service Password: <S: 0,82>

Specifies the password used by the VCS to log in and query the remote service. The maximum plaintext length is 30 characters, which will then be encrypted.

Example: **xConfiguration Policy AdministratorPolicy Service Password: "password123"**

Policy AdministratorPolicy Service Path: <S: 0,255>

Specifies the URL of the remote service.

Example: **xConfiguration Policy AdministratorPolicy Service Path: "service"**

Policy AdministratorPolicy Service Protocol: <HTTP/HTTPS>

Specifies the protocol used to connect to the remote service.

Default: HTTP

Example: **xConfiguration Policy AdministratorPolicy Service Protocol: HTTP**

Policy AdministratorPolicy Service Server [1..3] Address: <S: 0,128>

Specifies the IP address or Fully Qualified Domain Name (FQDN) of the remote service.

Example: `xConfiguration Policy AdministratorPolicy Service Server 1 Address: "service.server.example.com"`

Policy AdministratorPolicy Service TLS CRLCheck Mode: <On/Off>

Controls certificate revocation list checking of the certificate supplied by the policy service. When enabled, the server's X.509 certificate will be checked against the revocation list of the certificate authority of the certificate.

Default: Off

Example: `xConfiguration Policy AdministratorPolicy Service TLS CRLCheck Mode: Off`

Policy AdministratorPolicy Service TLS Verify Mode: <On/Off>

Controls X.509 certificate checking and mutual authentication between this VCS and the policy service. When enabled, the server's FQDN or IP address, as specified in the address field, must be contained within the server's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes).

Default: On

Example: `xConfiguration Policy AdministratorPolicy Service TLS Verify Mode: On`

Policy AdministratorPolicy Service UserName: <S: 0,30>

Specifies the user name used by the VCS to log in and query the remote policy service.

Example: `xConfiguration Policy AdministratorPolicy Service UserName: "user123"`

Policy FindMe CallerID: <FindMeID/IncomingID>

Determines how the source of an incoming call is presented to the callee.

IncomingID: displays the address of the endpoint from which the call was placed.

FindMeID: displays the FindMe ID associated with the originating endpoint's address.

Default: IncomingID

Example: `xConfiguration Policy FindMe CallerId: FindMeID`

Policy FindMe Mode: <Off/On/ThirdPartyManager>

Configures how the FindMe application operates.

Off: disables FindMe.

On: enables FindMe.

ThirdPartyManager: uses an off-box, third-party FindMe manager.

Default: Off

Example: `xConfiguration Policy FindMe Mode: On`

Policy FindMe Server Address: <S: 0, 128>

Specifies the IP address or Fully Qualified Domain Name (FQDN) of the remote FindMe Manager.

Example: `xConfiguration Policy FindMe Server Address: "userpolicy.server.example.com"`

Policy FindMe Server Password: <S: 0, 82>

Specifies the password used by the VCS to log in and query the remote FindMe Manager. The maximum plaintext length is 30 characters, which will then be encrypted.

Example: `xConfiguration Policy FindMe Server Password: "password123"`

Policy FindMe Server Path: <S: 0, 255>

Specifies the URL of the remote FindMe Manager.

Example: `xConfiguration Policy FindMe Server Path: "service"`

Policy FindMe Server Protocol: <HTTP/HTTPS>

Specifies the protocol used to connect to the remote FindMe Manager.

Default: HTTP

Example: `xConfiguration Policy FindMe Server Protocol: HTTP`

Policy FindMe Server UserName: <S: 0, 30>

Specifies the user name used by the VCS to log in and query the remote FindMe Manager.

Example: `xConfiguration Policy FindMe Server UserName: "user123"`

Policy FindMe UserDeviceRestriction: <Off/On>

Controls if users are restricted from adding, deleting or modifying their own devices.

Default: Off

Example: `xConfiguration Policy FindMe UserDeviceRestriction: Off`

Policy Services Service [1..5] DefaultCPL: <S: 0,255>

The CPL used by the VCS when the remote service is unavailable.

Default:

Example: `xConfiguration Policy Services Service 1 DefaultCPL: "<reject status='403' reason='Service Unavailable'/>"`

Policy Services Service [1..5] Description: <S: 0,64>

A free-form description of the Policy Service.

Example: `xConfiguration Policy Services Service 1 Description: "Conference management service"`

Policy Services Service [1..5] Name: <S: 0,50>

Assigns a name to this Policy Service.

Example: `xConfiguration Policy Services Service 1 Name: "Conference handler"`

Policy Services Service [1..5] Password: <S: 0,82>

Specifies the password used by the VCS to log in and query the remote service. The maximum plaintext length is 30 characters, which will then be encrypted.

Example: `xConfiguration Policy Services Service 1 Password: "password123"`

Policy Services Service [1..5] Path: <S: 0,255>

Specifies the URL of the remote service.

Example: `xConfiguration Policy Services Service 1 Path: "service"`

Policy Services Service [1..5] Protocol: <HTTP/HTTPS>

Specifies the protocol used to connect to the remote service.

Default: HTTP

Example: `xConfiguration Policy Services Service 1 Protocol: HTTP`

Policy Services Service [1..5] Server [1..3] Address: <S: 0,128>

Specifies the IP address or Fully Qualified Domain Name (FQDN) of the remote service.

Example: `xConfiguration Policy Services Service 1 Server 1 Address: "192.168.0.0"`

Policy Services Service [1..5] TLS CRLCheck Mode: <On/Off>

Controls certificate revocation list checking of the certificate supplied by the policy service. When enabled, the server's X.509 certificate will be checked against the revocation list of the certificate authority of the certificate.

Default: Off

Example: `xConfiguration Policy Services Service 1 TLS CRLCheck Mode: Off`

Policy Services Service [1..5] TLS Verify Mode: <On/Off>

Controls X.509 certificate checking and mutual authentication between this VCS and the policy service. When enabled, the server's FQDN or IP address, as specified in the address field, must be contained within the server's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes).

Default: On

Example: `xConfiguration Policy Services Service [1..5] TLS Verify Mode: On`

Policy Services Service [1..5] UserName: <S: 0,30>

Specifies the user name used by the VCS to log in and query the remote service.

Example: `xConfiguration Policy Services Service 1 UserName: "user123"`

Registration AllowList [1..2500] Description: <S: 0,64>

A free-form description of the Allow List rule.

Example: `xConfiguration Registration AllowList [1..2500] Description: "Everybody at @example.com"`

Registration AllowList [1..2500] Pattern String: <S: 0, 60>

Specifies an entry to be added to the Allow List. If one of an endpoint's aliases matches one of the patterns in the Allow List, the registration will be permitted.

Example: `xConfiguration Registration AllowList 1 Pattern String: "john.smith@example.com"`

Registration AllowList [1..2500] Pattern Type: <Exact/Prefix/Suffix/Regex>

Specifies whether the entry in the Allow List is a prefix, suffix, regular expression, or must be matched exactly.

Exact: the string must match the alias character for character.

Prefix: the string must appear at the beginning of the alias.

Suffix: the string must appear at the end of the alias.

Regex: the string will be treated as a regular expression.

Default: Exact

Example: `xConfiguration Registration AllowList 1 Pattern Type: Exact`

Registration DenyList [1..2500] Description: <S: 0,64>

A free-form description of the Deny List rule.

Example: `xConfiguration Registration DenyList [1..2500] Description: "Anybody at @nuisance.com"`

Registration DenyList [1..2500] Pattern String: <S: 0, 60>

Specifies an entry to be added to the Deny List. If one of an endpoint's aliases matches one of the patterns in the Deny List, the registration will not be permitted.

Example: **xConfiguration Registration DenyList 1 Pattern String: "john.jones@example.com"**

Registration DenyList [1..2500] Pattern Type: <Exact/Prefix/Suffix/Regex>

Specifies whether the entry in the Deny List is a prefix, suffix, regular expression, or must be matched exactly.

Exact: the string must match the alias character for character.

Prefix: the string must appear at the beginning of the alias.

Suffix: the string must appear at the end of the alias.

Regex: the string will be treated as a regular expression.

Default: Exact

Example: **xConfiguration Registration DenyList 1 Pattern Type: Exact**

Registration RestrictionPolicy Mode: <None/AllowList/DenyList/Directory/PolicyService>

Specifies the policy to be used when determining which endpoints may register with the system.

None: no restriction.

AllowList: only endpoints attempting to register with an alias listed on the Allow List may register.

DenyList: all endpoints, except those attempting to register with an alias listed on the Deny List, may register.

Directory: only endpoints who register an alias listed in the local Directory, may register.

PolicyService: only endpoints who register with details allowed by the Policy Service, may register.

Default: None

Example: **xConfiguration Registration RestrictionPolicy Mode: None**

Registration RestrictionPolicy Service DefaultCPL: <S: 0,255>

The CPL used by the VCS when the remote service is unavailable.

Default:

Example: **xConfiguration Registration RestrictionPolicy Service DefaultCPL: "<reject status='403' reason='Service Unavailable'/>"**

Registration RestrictionPolicy Service Password: <S: 0,82>

Specifies the password used by the VCS to log in and query the remote service. The maximum plaintext length is 30 characters, which will then be encrypted.

Example: **xConfiguration Registration RestrictionPolicy Service Password: "password123"**

Registration RestrictionPolicy Service Path: <S: 0,255>

Specifies the URL of the remote service.

Example: **xConfiguration Registration RestrictionPolicy Service Path: "service"**

Registration RestrictionPolicy Service Protocol: <HTTP/HTTPS>

Specifies the protocol used to connect to the remote service.

Default: HTTP

Example: **xConfiguration Registration RestrictionPolicy Service Protocol: HTTP**

Registration RestrictionPolicy Service Server [1..3] Address: <S: 0,128>

Specifies the IP address or Fully Qualified Domain Name (FQDN) of the remote service.

Example: `xConfiguration Registration RestrictionPolicy Service Server 1 Address: "192.168.0.0"`

Registration RestrictionPolicy Service TLS CRLCheck Mode: <On/Off>

Controls certificate revocation list checking of the certificate supplied by the policy service. When enabled, the server's X.509 certificate will be checked against the revocation list of the certificate authority of the certificate.

Default: Off

Example: `xConfiguration Registration RestrictionPolicy Service TLS CRLCheck Mode: Off`

Registration RestrictionPolicy Service TLS Verify Mode: <On/Off>

Controls X.509 certificate checking and mutual authentication between this VCS and the policy service. When enabled, the server's FQDN or IP address, as specified in the address field, must be contained within the server's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes).

Default: On

Example: `xConfiguration Registration RestrictionPolicy Service TLS Verify Mode: On`

Registration RestrictionPolicy Service UserName: <S: 0,30>

Specifies the user name used by the VCS to log in and query the remote service.

Example: `xConfiguration Registration RestrictionPolicy Service UserName: "user123"`

ResourceUsage Warning Activation Level: <0..100>

Controls if and when the VCS will warn that it is approaching its maximum licensed capacity for calls or registrations. The number represents the percentage of the maximum that, when reached, will trigger a warning. 0: Warnings will never appear.

Default: 90

Example: `xConfiguration ResourceUsage Warning Activation Level: 90`

SIP Authentication Digest Nonce ExpireDelta: <30..3600>

Specifies the maximum time (in seconds) that a nonce may be re-used for.

Default: 300

`Example: xConfiguration SIP Authentication Digest Nonce ExpireDelta: 300`

SIP Authentication Digest Nonce Length: <32..512>

Length of nonce or cnonce to generate for use in SIP Digest authentication.

Default: 60

Example: `xConfiguration SIP Authentication Digest Nonce Length: 60`

SIP Authentication Digest Nonce Limit: <1..65535>

Maximum limit on the number of nonces to store.

Default: 10000

Example: `xConfiguration SIP Authentication Digest Nonce Limit: 10000`

SIP Authentication Digest Nonce Maximum Use Count: <1..1024>

Maximum number of times that a nonce generated by the VCS may be used by a client.

Default: 128

Example: `xConfiguration SIP Authentication Digest Nonce Maximum Use Count: 128`

SIP Authentication NTLM Mode: <On/Off/Auto>

Controls when the VCS will challenge endpoints using the NTLM protocol.

Off: the VCS will never send a challenge containing the NTLM protocol.

On: the VCS will always include NTLM in its challenges.

Auto: the VCS will decide based on endpoint type whether to challenge with NTLM.

Default: Auto

Example: `xConfiguration SIP Authentication NTLM Mode: Auto`

SIP Authentication Retry Limit: <1..16>

The number of times a SIP UA will be challenged due to authentication failure before receiving a 403 Forbidden response.

Default: 3

Example: `xConfiguration SIP Authentication Retry Limit: 3`

Services AdvancedMediaGateway Policy Mode: <On/Off>

Controls whether the policy rules are used to control access to the Advanced Media Gateway.

Default: Off

Example: `xConfiguration Services AdvancedMediaGateway Policy Mode: On`

Services AdvancedMediaGateway Policy Rules Rule [1..200] Action: <Allow/Deny>

The action to take if the source or destination alias of the call matches this policy rule.

Allow: the call can connect via the Advanced Media Gateway.

Deny: the call can connect but it will not use Advanced Media Gateway resources.

Default: Allow

Example: `xConfiguration Services AdvancedMediaGateway Policy Rules Rule 1 Action: Allow`

Services AdvancedMediaGateway Policy Rules Rule [1..200] Description: <S: 0,64>

A free-form description of the Advanced Media Gateway policy rule.

Example: `xConfiguration Services AdvancedMediaGateway Policy Rules Rule 1 Description: "Deny all calls to branch office"`

Services AdvancedMediaGateway Policy Rules Rule [1..200] Name: <S: 0,50>

Assigns a name to this Advanced Media Gateway policy rule.

Example: `xConfiguration Services AdvancedMediaGateway Policy Rules Rule 1 Name: "Deny branch calls"`

Services AdvancedMediaGateway Policy Rules Rule [1..200] Pattern String: <S: 0,60>

The pattern against which the alias is compared.

Example: `xConfiguration Services AdvancedMediaGateway Policy Rules Rule 1 Pattern String: ".branch@example.com"`

Services AdvancedMediaGateway Policy Rules Rule [1..200] Pattern Type: <Exact/Prefix/Suffix/Regex>

The way in which the pattern must match either the source or destination alias of the call.

Exact: the entire pattern string must exactly match the alias character for character.

Prefix: the pattern string must appear at the beginning of the alias.

Suffix: the pattern string must appear at the end of the alias.

Regex: the pattern string is treated as a regular expression.

Default: Exact

Example: **xConfiguration Services AdvancedMediaGateway Policy Rules Rule 1 Pattern Type: Suffix**

Services AdvancedMediaGateway Policy Rules Rule [1..200] Priority: <1..65534>

Determines 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. If multiple rules have the same priority they are applied in configuration order.

Default: 100

Example: **xConfiguration Services AdvancedMediaGateway Policy Rules Rule 1 Priority: 50**

Services AdvancedMediaGateway Policy Rules Rule [1..200] State: <Enabled/Disabled>

Indicates if the policy rule is enabled or disabled. Disabled policy rules are ignored.

Default: Enabled

Example: **xConfiguration Services AdvancedMediaGateway Policy Rules Rule 1 State: Enabled**

Services AdvancedMediaGateway Zone Name: <S: 0,50>

The zone used by the VCS to connect to one or more Advanced Media Gateways.

Example: **xConfiguration Services AdvancedMediaGateway Zone Name: "AM gateway zone"**

SIP Domains Domain [1..20] Name: <S: 0,128>

Specifies a domain for which this VCS is authoritative. The VCS will act as a SIP registrar and Presence Server for this domain, and will accept registration requests for any SIP endpoints attempting to register with an alias that includes this domain. The domain name can comprise multiple levels. Each level's name can only contain letters, digits and hyphens, with each level separated by a period (dot). A level name cannot start or end with a hyphen, and the final level name must start with a letter. An example valid domain name is "100.example-name.com".

Example: **xConfiguration SIP Domains Domain 1 Name: "100.example-name.com"**

SIP Mode: <On/Off>

Determines whether or not the VCS will provide SIP registrar and SIP proxy functionality. This mode must be enabled in order to use either the Presence Server or the Presence User Agent.

Default: On

Example: **xConfiguration SIP Mode: On**

SIP Registration Call Remove: <Yes/No>

Specifies whether associated calls are dropped when a SIP registration expires or is removed.

Default: No

Example: **xConfiguration SIP Registration Call Remove: No**

SIP Registration ExpireDelta: <30..7200>

Specifies the period (in seconds) within which a SIP endpoint must re-register with the VCS to prevent its registration expiring.

Default: 60

Example: **xConfiguration SIP Registration ExpireDelta: 60**

SIP Registration Proxy Mode: <Off/ProxyToKnownOnly/ProxyToAny>

Specifies how proxied registrations should be handled.

Off: registration requests will not be proxied.

ProxyToKnownOnly: registration requests will be proxied to neighbors only.

ProxyToAny: registration requests will be proxied in accordance with the VCS's existing call processing rules.

Default: Off

Example: **xConfiguration SIP Registration Proxy Mode: Off**

SIP Require Duo Video Mode: <On/Off>

Controls whether the VCS will require the use of the com.tandberg.sdp.duo.enable extension for endpoints that support it.

Default: On

Example: **xConfiguration SIP Require Duo Video Mode: On**

SIP Require UDP BFCP Mode: <On/Off>

Controls whether the VCS will require the use of the com.tandberg.udp.bfcp extension for endpoints that support it.

Default: On

Example: **xConfiguration SIP Require UDP BFCP Mode: On**

SIP Routes Route [1..20] Address: <S:0,39>

Specifies the IP address of the next hop for this route, where matching SIP requests will be forwarded.

Note: this command is intended for developer use only.

Example: **xConfiguration SIP Routes Route 1 Address: "127.0.0.1"**

SIP Routes Route [1..20] Authenticated: <On/Off>

Whether to forward authenticated requests.

On: only forward requests along route if incoming message has been authenticated.

Off: always forward messages that match this route.

Default: Off

Note: this command is intended for developer use only.

Example: **xConfiguration SIP Routes Route 1 Authenticated: On**

SIP Routes Route [1..20] Header Name: <S:0,64>

Name of SIP header field to match (e.g. Event).

Note: this command is intended for developer use only.

Example: **xConfiguration SIP Routes Route 1 Header Name: "Event"**

SIP Routes Route [1..20] Header Pattern: <S:0,128>

Regular expression to match against the specified SIP header field.

Note: this command is intended for developer use only.

Example: `xConfiguration SIP Routes Route 1 Header Pattern: "(my-event-package)(.*)"`

SIP Routes Route [1..20] Method: <S:0,64>

SIP method to match to select this route (e.g. INVITE, SUBSCRIBE).

Note: this command is intended for developer use only.

Example: `xConfiguration SIP Routes Route 1 Method: "SUBSCRIBE"`

SIP Routes Route [1..20] Port: <1..65534>

Specifies the port on the next hop for this route to which matching SIP requests will be routed.

Default: 5060

Note: this command is intended for developer use only.

Example: `xConfiguration SIP Routes Route 1 Port: 22400`

SIP Routes Route [1..20] Request Line Pattern: <S:0,128>

Regular expression to match against the SIP request line.

Note: this command is intended for developer use only.

Example: `xConfiguration SIP Routes Route 1 Request Line Pattern: ".*@(%localdomains%|%ip%)"`

SIP Routes Route [1..20] Tag: <S:0,64>

Tag value specified by external applications to identify routes that they create.

Note: this command is intended for developer use only.

Example: `xConfiguration SIP Routes Route 1 Tag: "Tag1"`

SIP Routes Route [1..20] Transport: <UDP/TCP/TLS>

Determines which transport type will be used for SIP messages forwarded along this route.

Default: TCP

Note: this command is intended for developer use only.

Example: `xConfiguration SIP Routes Route 1 Transport: TCP`

SIP Session Refresh Minimum: <90..7200>

The minimum value the VCS will negotiate for the session refresh interval for SIP calls. For further information refer to the definition of Min-SE header in RFC 4028.

Default: 500

Example: `xConfiguration SIP Session Refresh Minimum: 500`

SIP Session Refresh Value: <90..7200>

The maximum time allowed between session refresh requests for SIP calls. For further information refer to the definition of Session-Expires in RFC 4028.

Default: 1800

Example: `xConfiguration SIP Session Refresh Value: 1800`

SIP TCP Mode: <On/Off>

Determines whether incoming and outgoing SIP calls using the TCP protocol will be allowed.

Default: On

Example: `xConfiguration SIP TCP Mode: On`

SIP TCP Outbound Port End: <1024..65534>

Specifies the upper port in the range to be used by outbound TCP/TLS SIP connections.

Default: 29999

Example: `xConfiguration SIP TCP Outbound Port End: 29999`

SIP TCP Outbound Port Start: <1024..65534>

Specifies the lower port in the range to be used by outbound TCP/TLS SIP connections.

Default: 25000

Example: `xConfiguration SIP TCP Outbound Port Start: 25000`

SIP TCP Port: <1024..65534>

Specifies the listening port for incoming SIP TCP calls.

Default: 5060

Example: `xConfiguration SIP TCP Port: 5060`

SIP TLS Mode: <On/Off>

Determines whether incoming and outgoing SIP calls using the TLS protocol will be allowed.

Default: On

Example: `xConfiguration SIP TLS Mode: On`

SIP TLS Port: <1024..65534>

Specifies the listening port for incoming SIP TLS calls.

Default: 5061

Example: `xConfiguration SIP TLS Port: 5061`

SIP UDP Mode: <On/Off>

Determines whether incoming and outgoing SIP calls using the UDP protocol will be allowed.

Default: On

Example: `xConfiguration SIP UDP Mode: On`

SIP UDP Port: <1024..65534>

Specifies the listening port for incoming SIP UDP calls.

Default: 5060

Example: `xConfiguration SIP UDP Port: 5060`

SNMP CommunityName: <S: 0, 16>

Sets the VCS's SNMP community name.

Default: public

Example: `xConfiguration SNMP CommunityName: "public"`

SNMP Mode: <On/Off>

Enables or disables SNMP support.

Default: Off

Example: `xConfiguration SNMP Mode: On`

SNMP SystemContact: <S: 0, 70>

Specifies the name of the person who can be contacted regarding issues with the VCS.

Example: `xConfiguration SNMP SystemContact: "John Smith"`

SNMP SystemLocation: <S: 0, 70>

Specifies the physical location of the VCS.

Example: `xConfiguration SNMP SystemLocation: "Server Room 128"`

SNMP V1 Mode: <On/Off>

Enables or disables SNMP Version 1 support.

Default: On

Example: `xConfiguration SNMP V1 Mode: On`

SNMP V2c Mode: <On/Off>

Enables or disables SNMP Version 2c support.

Default: On

Example: `xConfiguration SNMP V2c Mode: On`

SNMP V3 Authentication Mode: <On/Off>

Enables or disables SNMP Version 3 authentication.

Default: On

Example: `xConfiguration SNMP V3 Authentication Mode: On`

SNMP V3 Authentication Password: <S: 0,215>

Sets SNMP Version 3 authentication password. Note: must be at least 8 characters.

Example: `xConfiguration SNMP V3 Authentication Password: "password123"`

SNMP V3 Authentication Type: <MD5/SHA>

Sets SNMP Version 3 authentication type.

Example: `xConfiguration SNMP V3 Authentication Type: SHA`

SNMP V3 Mode: <On/Off>

Enables or disables SNMP Version 3 support.

Default: On

Example: `xConfiguration SNMP V3 Mode: On`

SNMP V3 Privacy Mode: <On/Off>

Enables or disables SNMP Version 3 privacy.

Default: On

Example: `xConfiguration SNMP V3 Privacy Mode: On`

SNMP V3 Privacy Password: <S: 0,215>

Sets SNMP Version 3 privacy password. Note: must be at least 8 characters.

Example: `xConfiguration SNMP V3 Privacy Password: "password123"`

SNMP V3 Privacy Type: <DES/AES>

Sets SNMP Version 3 privacy type.

Example: `xConfiguration SNMP V3 Privacy Type: AES`

SNMP V3 UserName: <S: 0,70>

Sets the username to use when using SNMP V3.

Example: `xConfiguration SNMP V3 UserName: "user123"`

SystemUnit AdminAccount [1..15] Access: <AccountDisabled/ReadOnly/ReadWrite/Auditor >

Defines the access level of an administrator user who can login to the VCS web interface.

AccountDisabled: no access allowed.

ReadOnly: configuration can only be viewed.

ReadWrite: configuration can be viewed and changed.

Auditor: allows access to the Event Log, Configuration Log and the Overview page only.

Default: ReadWrite

Example: `xConfiguration SystemUnit AdminAccount 1 Access: ReadOnly`

SystemUnit AdminAccount [1..15] Name: <S:0,25>

Defines the name of an administrator user who can login to the VCS web interface.

Example: `xConfiguration SystemUnit AdminAccount 1 Name: "guest"`

SystemUnit AdminAccount [1..15] Password: <S:0,65>

Defines the password of an administrator user who can login to the VCS web interface. The maximum plaintext length is 16 characters, which will then be encrypted.

Example: `xConfiguration SystemUnit AdminAccount 1 Password: "password123"`

SystemUnit Maintenance Mode: <On/Off>

Sets the VCS into maintenance mode. New calls and registrations are disallowed and existing registrations are allowed to expire.

Default: Off

Example: `xConfiguration SystemUnit Maintenance Mode: Off`

SystemUnit Name: <S:, 0, 50>

Defines the name of the VCS. Choose a name that uniquely identifies the system.

Example: `xConfiguration SystemUnit Name: "VCS HQ"`

SystemUnit Password: <S: 0, 65>

Defines the password for the default 'admin' account. This account is used to log in to the VCS via Telnet, HTTP(S), SSH, SCP, and on the serial port. The maximum plaintext length is 16 characters, which will then be encrypted.

Example: `xConfiguration SystemUnit Password: "password123"`

SystemUnit StrictPassword Enforce: <On/Off>

Determines whether or not administrator passwords must meet a certain level of complexity before they are accepted.

Default: Off

Example: **`xConfiguration SystemUnit StrictPassword Enforce: Off`**

TimeZone Name: <S: 0, 64>

Sets the local time zone of the VCS. Time zone names follow the POSIX naming convention e.g. Europe/London or America/New_York.

Default: GMT

Example: **`xConfiguration TimeZone Name: "GMT"`**

Transform [1..100] Description: <S: 0,64>

A free-form description of the transform.

Example: **`xConfiguration Transform [1..100] Description: "Change example.net to example.com"`**

Transform [1..100] Pattern Behavior: <Strip/Replace>

How the alias is modified.

Strip: removes the matching prefix or suffix from the alias.

Replace: substitutes the matching part of the alias with the text in replace string.

AddPrefix: prepends the replace string to the alias.

AddSuffix: appends the replace string to the alias.

Default: Strip

Example: **`xConfiguration Transform 1 Pattern Behavior: Replace`**

Transform [1..100] Pattern Replace: <S: 0, 60>

The text string to use in conjunction with the selected Pattern behavior.

Example: **`xConfiguration Transform 1 Pattern Replace: "example.com"`**

Transform [1..100] Pattern String: <S: 0, 60>

The pattern against which the alias is compared.

Example: **`xConfiguration Transform 1 Pattern String: "example.net"`**

Transform [1..100] Pattern Type: <Exact/Prefix/Suffix/Regex>

How the pattern string must match the alias for the transform to be applied.

Exact: the entire string must exactly match the alias character for character.

Prefix: the string must appear at the beginning of the alias.

Suffix: the string must appear at the end of the alias.

Regex: the string is treated as a regular expression.

Default: Prefix

Example: **`xConfiguration Transform 1 Pattern Type: Suffix`**

Transform [1..100] Priority: <1..65534>

Assigns a priority to the specified transform. Transforms are compared with incoming aliases in order of priority, and the priority must be unique for each transform.

Default: 1

Example: `xConfiguration Transform 1 Priority: 10`

Transform [1..100] State: <Enabled/Disabled>

Indicates if the transform is enabled or disabled. Disabled transforms are ignored.

Example: `xConfiguration Transform 1 State: Enabled`

Traversal Media Port End: <1025..65533>

For traversal calls (i.e. where the VCS is taking the media as well as the signaling), specifies the upper port in the range to be used for the media. Ports are allocated from this range in pairs, the first of each being even. Therefore the range must end with an odd number.

Default: 52399

Example: `xConfiguration Traversal Media Port End: 52399`

Traversal Media Port Start: <1024..65532>

For traversal calls (i.e. where the VCS is taking the media as well as the signaling), specifies the lower port in the range to be used for the media. Ports are allocated from this range in pairs, the first of each being even. Therefore the range must start with an even number.

Default: 50000

Example: `xConfiguration Traversal Media Port Start: 50000`

Traversal Server H323 Assent CallSignaling Port: <1024..65534>

Specifies the port on the VCS to be used for Assent signaling.

Default: 2776

Example: `xConfiguration Traversal Server H323 Assent CallSignaling Port: 2777`

Traversal Server H323 H46018 CallSignaling Port: <1024..65534>

Specifies the port on the VCS to be used for H460.18 signaling.

Default: 2777

Example: `xConfiguration Traversal Server H323 H46018 CallSignaling Port: 2777`

Traversal Server Media Demultiplexing RTCP Port: <1024..65534>

Specifies the port on the VCS to be used for demultiplexing RTCP media. Note: You must restart the system for any changes to take effect.

Default: 2777

Example: `xConfiguration Traversal Server Media Demultiplexing RTCP Port: 2777`

Traversal Server Media Demultiplexing RTP Port: <1024..65534>

Specifies the port on the VCS to be used for demultiplexing RTP media. Note: You must restart the system for any changes to take effect.

Default: 2776

Example: `xConfiguration Traversal Server Media Demultiplexing RTP Port: 2776`

Traversal Server TURN Authentication Realm: <S: 1,128>

The realm sent by the server in its authentication challenges.

Default: TANDBERG

Example: **xConfiguration Traversal Server TURN Authentication Realm: "TANDBERG"**

Traversal Server TURN Media Port End: <1024..65534>

The upper port in the range used for TURN relays.

Default: 61399

Example: **xConfiguration Traversal Server TURN Media Port End: 61399**

Traversal Server TURN Media Port Start: <1024..65534>

The lower port in the range used for TURN relays.

Default: 60000

Example: **xConfiguration Traversal Server TURN Media Port Start: 60000**

Traversal Server TURN Mode: <On/Off>

Determines whether the VCS offers TURN services to traversal clients.

Default: Off

Example: **xConfiguration Traversal Server TURN Mode: Off**

Traversal Server TURN Port: <1024..65534>

The listening port for TURN requests.

Default: 3478

Example: **xConfiguration Traversal Server TURN Port: 3478**

Zones DefaultZone Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

Controls how the VCS authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. See the Administrator Guide for full details about each of the Authentication Policy options.

Default: DoNotCheckCredentials

Example: **xConfiguration Zones DefaultZone Authentication Mode: DoNotCheckCredentials**

Zones LocalZone DefaultSubZone Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

Controls how the VCS authenticates incoming messages from this subzone and whether they are subsequently treated as authenticated, unauthenticated or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. See the Administrator Guide for further information.

Default: DoNotCheckCredentials

Example: **xConfiguration Zones LocalZone DefaultSubZone Authentication Mode: DoNotCheckCredentials**

Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Limit: <1..100000000>

Specifies the bandwidth limit (in kbps) for any one call to or from an endpoint in the Default Subzone (applies only if the mode is set to Limited).

Default: 1920

Example: **xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Limit: 1920**

Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Mode: <Limited/Unlimited/NoBandwidth>

Determines whether there is a limit on the bandwidth for any one call to or from an endpoint in the Default Subzone.

NoBandwidth: no bandwidth available. No calls can be made to or from the Default Subzone.

Default: Unlimited

Example: **xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Mode: Limited**

Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Limit: <1..100000000>

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

Example: **xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Limit: 1920**

Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Mode: <Limited/Unlimited/NoBandwidth>

Determines whether there is a limit on the bandwidth for any one call between two endpoints within the Default Subzone.

NoBandwidth: no bandwidth available. No calls can be made within the Default Subzone.

Default: Unlimited

Example: **xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Mode: Limited**

Zones LocalZone DefaultSubZone Bandwidth Total Limit: <1..100000000>

Sets the total bandwidth limit (in kbps) of the Default Subzone (applies only if Mode is set to Limited).

Default: 500000

Example: **xConfiguration Zones LocalZone DefaultSubZone Bandwidth Total Limit: 500000**

Zones LocalZone DefaultSubZone Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth>

Determines whether the Default Subzone has a limit on the total bandwidth being used by its endpoints at any one time.

NoBandwidth: no bandwidth available. No calls can be made to, from, or within the Default Subzone.

Default: Unlimited

Example: **xConfiguration Zones LocalZone DefaultSubZone Bandwidth Total Mode: Limited**

Zones LocalZone DefaultSubZone Registrations: <Allow/Deny>

Controls whether registrations assigned to the Default Subzone are accepted.

Default: Allow

Example: **xConfiguration Zones LocalZone DefaultSubZone Registrations: Allow**

Zones LocalZone SubZones MembershipRules Rule [1..3000] Description: <S: 0,64>

A free-form description of the membership rule.

Example: `xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Description: "Office-based staff"`

Zones LocalZone SubZones MembershipRules Rule [1..3000] Name: <S: 0,50>

Assigns a name to this membership rule.

Example: `xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Name: "Office Workers"`

Zones LocalZone SubZones MembershipRules Rule [1..3000] Pattern String: <S: 0,60>

Specifies the pattern against which the alias is compared.

Example: `xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Pattern String: "@example.com"`

Zones LocalZone SubZones MembershipRules Rule [1..3000] Pattern Type: <Exact/Prefix/Suffix/Regex>

The way in which the pattern must match the alias.

Example: `xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Pattern Type: Suffix`

Zones LocalZone SubZones MembershipRules Rule [1..3000] Priority: <1..65534>

Determines the order in which the rules are applied (and thus to which subzone the endpoint is assigned) if an endpoint's address satisfies multiple rules. The rules with the highest priority (1, then 2, then 3 and so on) are applied first. If multiple Subnet rules have the same priority the rule with the largest prefix length is applied first. Alias Pattern Match rules at the same priority are searched in configuration order.

Default: 100

Example: `xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Priority: 100`

Zones LocalZone SubZones MembershipRules Rule [1..3000] State: <Enabled/Disabled>

Indicates if the membership rule is enabled or disabled. Disabled membership rules are ignored.

Default: Enabled

Example: `xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 State: Enabled`

Zones LocalZone SubZones MembershipRules Rule [1..3000] SubZoneName: <S: 0,50>

The subzone to which an endpoint is assigned if its address satisfies this rule.

Example: `xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 SubZoneName: "Branch Office"`

Zones LocalZone SubZones MembershipRules Rule [1..3000] Subnet Address: <S: 0,39>

Specifies an IP address used (in conjunction with the prefix length) to identify this subnet.

Example: `xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Subnet Address: "192.168.0.0"`

Zones LocalZone SubZones MembershipRules Rule [1..3000] Subnet PrefixLength: <1..128>

The number of bits of the subnet address which must match for an IP address to belong in this subnet.

Default: 32

Example: **xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Subnet PrefixLength: 32**

Zones LocalZone SubZones MembershipRules Rule [1..3000] Type: <Subnet/AliasPatternMatch>

The type of address that applies to this rule.

Subnet: assigns the device if its IP address falls within the configured IP address subnet.

AliasPatternMatch: assigns the device if its alias matches the configured pattern.

Example: **xConfiguration Zones LocalZone SubZones MembershipRules Rule 1 Type: Subnet**

Zones LocalZone SubZones SubZone [1..1000] Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

Controls how the VCS authenticates incoming messages from this subzone and whether they are subsequently treated as authenticated, unauthenticated or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. See the Administrator Guide for further information.

Default: DoNotCheckCredentials

Example: **xConfiguration Zones LocalZone SubZones SubZone 1 Authentication Mode: DoNotCheckCredentials**

Zones LocalZone SubZones SubZone [1..1000] Bandwidth PerCall Inter Limit: <1..100000000>

Specifies the bandwidth limit (in kbps) on any one call to or from an endpoint in this subzone (applies only if Mode is set to Limited).

Default: 1920

Example: **xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth PerCall Inter Limit: 1920**

Zones LocalZone SubZones SubZone [1..1000] Bandwidth PerCall Inter Mode: <Limited/Unlimited/NoBandwidth>

Determines whether there is a limit on the bandwidth for any one call to or from an endpoint in this subzone.

NoBandwidth: no bandwidth available. No calls can be made to or from this subzone.

Default: Unlimited

Example: **xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth PerCall Inter Mode: Limited**

Zones LocalZone SubZones SubZone [1..1000] Bandwidth PerCall Intra Limit: <1..100000000>

Specifies the bandwidth limit (in kbps) for any one call between two endpoints within this subzone (applies only if the mode is set to Limited).

Default: 1920

Example: **Zones LocalZone SubZones SubZone 1 Bandwidth PerCall Intra Limit: 1920**

Zones LocalZone SubZones SubZone [1..1000] Bandwidth PerCall Intra Mode: <Limited/Unlimited/NoBandwidth>

Determines whether there is a limit on the bandwidth for any one call between two endpoints within this subzone.

NoBandwidth: no bandwidth available. No calls can be made within this subzone.

Default: Unlimited

Example: **xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth PerCall Intra Mode: Limited**

Zones LocalZone SubZones SubZone [1..1000] Bandwidth Total Limit: <1..100000000>

Sets the total bandwidth limit (in kbps) of this subzone (applies only if the mode is set to Limited).

Default: 500000

Example: **xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth Total Limit: 500000**

Zones LocalZone SubZones SubZone [1..1000] Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth>

Determines whether this subzone has a limit on the total bandwidth of calls being used by its endpoints at any one time.

NoBandwidth: no bandwidth available. No calls can be made to, from, or within this subzone.

Default: Unlimited

Example: **xConfiguration Zones LocalZone SubZones SubZone 1 Bandwidth Total Mode: Limited**

Zones LocalZone SubZones SubZone [1..1000] Name: <S: 0, 50>

Assigns a name to this subzone.

Example: **xConfiguration Zones LocalZone SubZones SubZone 1 Name: "BranchOffice"**

Zones LocalZone SubZones SubZone [1..1000] Registrations: <Allow/Deny>

Controls whether registrations assigned to this subzone are accepted.

Default: Allow

Example: **xConfiguration Zones LocalZone SubZones SubZone 1 Registrations: Allow**

Zones LocalZone Traversal H323 Assent Mode: <On/Off>

Determines whether or not H.323 calls using Assent mode for firewall traversal will be allowed. Applies to traversal-enabled endpoints registered directly with the VCS.

Default: On

Example: **xConfiguration Zones LocalZone Traversal H323 Assent Mode: On**

Zones LocalZone Traversal H323 H46018 Mode: <On/Off>

Determines whether or not H.323 calls using H460.18 mode for firewall traversal will be allowed. Applies to traversal-enabled endpoints registered directly with the VCS.

Default: On

Example: **xConfiguration Zones LocalZone Traversal H323 H46018 Mode: On**

Zones LocalZone Traversal H323 H46019 Demultiplexing Mode: <On/Off>

Determines whether the VCS will operate in Demultiplexing mode for calls from traversal-enabled endpoints registered directly with it.

On: allows use of the same two ports for all calls.

Off: each call will use a separate pair of ports for media.

Default: Off

Example: **xConfiguration Zones LocalZone Traversal H323 H46019 Demultiplexing Mode: Off**

Zones LocalZone Traversal H323 Preference: <Assent/H46018>

If an endpoint that is registered directly with the VCS supports both Assent and H460.18 protocols, this setting determines which the VCS uses.

Default: Assent

Example: **xConfiguration Zones LocalZone Traversal H323 Preference: Assent**

Zones LocalZone Traversal H323 TCPProbe KeepAliveInterval: <1..65534>

Sets the interval (in seconds) with which a traversal-enabled endpoint registered directly with the VCS will send a TCP probe to the VCS once a call is established, in order to keep the firewall's NAT bindings open.

Default: 20

Example: **xConfiguration Zones LocalZone Traversal H323 TCPProbe KeepAliveInterval: 20**

Zones LocalZone Traversal H323 TCPProbe RetryCount: <1..65534>

Sets the number of times traversal-enabled endpoints registered directly with the VCS will attempt to send a TCP probe to the VCS.

Default: 5

Example: **xConfiguration Zones LocalZone Traversal H323 TCPProbe RetryCount: 5**

Zones LocalZone Traversal H323 TCPProbe RetryInterval: <1..65534>

Sets the frequency (in seconds) with which traversal-enabled endpoints registered directly with the VCS will send a TCP probe to the VCS.

Default: 2

Example: **xConfiguration Zones LocalZone Traversal H323 TCPProbe RetryInterval: 2**

Zones LocalZone Traversal H323 UDPProbe KeepAliveInterval: <1..65534>

Sets the interval (in seconds) with which a traversal-enabled endpoint registered directly with the VCS will send a UDP probe to the VCS once a call is established, in order to keep the firewall's NAT bindings open.

Default: 20

Example: **xConfiguration Zones LocalZone Traversal H323 UDPProbe KeepAliveInterval: 20**

Zones LocalZone Traversal H323 UDPProbe RetryCount: <1..65534>

Sets the number of times traversal-enabled endpoints registered directly with the VCS will attempt to send a UDP probe to the VCS.

Default: 5

Example: **xConfiguration Zones LocalZone Traversal H323 UDPProbe RetryCount: 5**

Zones LocalZone Traversal H323 UDPProbe RetryInterval: <1..65534>

Sets the frequency (in seconds) with which traversal-enabled endpoints registered directly with the VCS will send a UDP probe to the VCS.

Default: 2

Example: **xConfiguration Zones LocalZone Traversal H323 UDPProbe RetryInterval: 2**

Zones LocalZone TraversalSubZone Bandwidth PerCall Limit: <1..100000000>

Specifies the bandwidth limit (in kbps) applied to any one traversal call being handled by the VCS (applies only if the mode is set to Limited).

Default: 1920

Example: **xConfiguration Zones LocalZone TraversalSubZone Bandwidth PerCall Limit: 1920**

Zones LocalZone TraversalSubZone Bandwidth PerCall Mode: <Limited/Unlimited/NoBandwidth>

Determines whether there is a limit on the bandwidth of any one traversal call being handled by the VCS.

NoBandwidth: no bandwidth available. No traversal calls can be made.

Default: Unlimited

Example: **xConfiguration Zones LocalZone TraversalSubZone Bandwidth PerCall Mode: Limited**

Zones LocalZone TraversalSubZone Bandwidth Total Limit: <1..100000000>

Specifies the total bandwidth (in kbps) allowed for all traversal calls being handled by the VCS (applies only if the mode is set to Limited).

Default: 500000

Example: **xConfiguration Zones LocalZone TraversalSubZone Bandwidth Total Limit: 500000**

Zones LocalZone TraversalSubZone Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth>

Determines whether or not there is a limit to the total bandwidth of all traversal calls being handled by the VCS.

NoBandwidth: no bandwidth available. No traversal calls can be made.

Default: Unlimited

Example: **xConfiguration Zones LocalZone TraversalSubZone Bandwidth Total Mode: Limited**

Zones Policy Mode: <SearchRules/Directory>

The mode used when attempting to locate a destination.

SearchRules: use the configured search rules to determine which zones are queried and in what order.

Directory: use the facilities of a directory service to direct the request to the correct zones.

Default: SearchRules

Example: **xConfiguration Zones Policy Mode: SearchRules**

Zones Policy SearchRules Rule [1..2000] Authentication: <Yes/No>

Specifies whether this search rule applies only to authenticated search requests.

Default: No

Example: **xConfiguration Zones Policy SearchRules Rule 1 Authentication: No**

Zones Policy SearchRules Rule [1..2000] Description: <S: 0,64>

A free-form description of the search rule.

Example: **xConfiguration Zones Policy SearchRules Rule 1 Description: "Send query to the DNS zone"**

Zones Policy SearchRules Rule [1..2000] Mode: <AliasPatternMatch/AnyAlias/AnyIPAddress>

Determines whether a query is sent to the target zone.

AliasPatternMatch: queries the zone only if the alias matches the corresponding pattern type and string.

AnyAlias: queries the zone for any alias (but not IP address).

AnyIPAddress: queries the zone for any given IP address (but not alias).

Default: AnyAlias

Example: **xConfiguration Zones Policy SearchRules Rule 1 Mode: AnyAlias**

Zones Policy SearchRules Rule [1..2000] Name: <S: 0,50>

Descriptive name for the search rule.

Example: **xConfiguration Zones Policy SearchRules Rule 1 Name: "DNS lookup"**

Zones Policy SearchRules Rule [1..2000] Pattern Behavior: <Strip/Leave/Replace>

Determines whether the matched part of the alias is modified before being sent to the target zone. (Applies to Alias Pattern Match mode only.)

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.

Default: Strip

Example: **xConfiguration Zones Policy SearchRules Rule 1 Pattern Behavior: Strip**

Zones Policy SearchRules Rule [1..2000] Pattern Replace: <S: 0,60>

The string to substitute for the part of the alias that matches the pattern. (Applies to Replace pattern behavior only.)

Example: **xConfiguration Zones Policy SearchRules Rule 1 Pattern Replace: "@example.net"**

Zones Policy SearchRules Rule [1..2000] Pattern String: <S: 0,60>

The pattern against which the alias is compared. (Applies to Alias Pattern Match mode only.)

Example: **xConfiguration Zones Policy SearchRules Rule 1 Pattern String: "@example.com"**

Zones Policy SearchRules Rule [1..2000] Pattern Type: <Exact/Prefix/Suffix/Regex>

How the pattern string must match the alias for the rule to be applied. (Applies to Alias Pattern Match mode only.)

Exact: the entire string must exactly match the alias character for character.

Prefix: the string must appear at the beginning of the alias.

Suffix: the string must appear at the end of the alias.

Regex: the string is treated as a regular expression.

Default: Prefix

Example: **xConfiguration Zones Policy SearchRules Rule 1 Pattern Type: Suffix**

Zones Policy SearchRules Rule [1..2000] Priority: <1..65534>

The order in the search process that this rule is applied, when compared to the priority of the other search rules. All Priority 1 search rules are applied first, followed by all Priority 2 search rules, and so on.

Default: 100

Example: **xConfiguration Zones Policy SearchRules Rule 1 Priority: 100**

Zones Policy SearchRules Rule [1..2000] Progress: <Continue/Stop>

Specifies the ongoing search behavior if the alias matches this search rule. If 'stop' is selected, any rules with the same priority level as this rule are still applied.

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.

Default: Continue

Example: **xConfiguration Zones Policy SearchRules Rule 1 Progress: Continue**

Zones Policy SearchRules Rule [1..2000] Source: <Any/AllZones/LocalZone>

The sources of the requests for which this rule applies.

Any: locally registered devices, neighbor or traversal zones, and any non-registered devices.

AllZones: locally registered devices plus neighbor or traversal zones.

LocalZone: locally registered devices only.

Default: Any

Example: **xConfiguration Zones Policy SearchRules Rule 1 Source: Any**

Zones Policy SearchRules Rule [1..2000] State: <Enabled/Disabled>

Indicates if the search rule is enabled or disabled. Disabled search rules are ignored.

Default: Enabled

Example: **xConfiguration Zones Policy SearchRules Rule 1 State: Enabled**

Zones Policy SearchRules Rule [1..2000] Target Name: <S: 0,50>

The zone or policy service to query if the alias matches the search rule.

Example: **xConfiguration Zones Policy SearchRules Rule 1 Target Name: "Sales Office"**

Zones Policy SearchRules Rule [1..2000] Target Type: <Zone/PolicyService>

The type of target this search rule applies to.

Example: **xConfiguration Zones Policy SearchRules Rule [1..2000] Target Type: Zone**

Zones Zone [1..1000] DNS IncludeAddressRecord: <On/Off>

Determines whether, if no NAPTR (SIP) or SRV (SIP and H.323) records have been found for the dialed alias via this zone, the VCS will then query for A and AAAA DNS Records.

Default: Off

Example: **xConfiguration Zones Zone 1 DNS IncludeAddressRecord: Off**

Zones Zone [1..1000] DNS Interworking SIP Audio DefaultCodec: <G711u/G711a/G722_48/G722_56/G722_64/G722_1_16/G722_1_24/G722_1_32/G722_1_48/G723_1/G728/G729/AALCD_48/AALCD_56/AALCD_64/AMR>

Specifies which audio codec to use when empty INVITEs are not allowed.

Default: G711u

Example: `xConfiguration Zones Zone 1 DNS Interworking SIP Audio DefaultCodec: G711u`

Zones Zone [1..1000] DNS Interworking SIP EmptyInviteAllowed: <On/Off>

Determines whether the VCS will generate a SIP INVITE message with no SDP to send to this zone. INVITEs with no SDP mean that the destination device is asked to initiate the codec selection, and are used when the call has been interworked locally from H.323.

On: SIP INVITEs with no SDP will be generated and sent to this neighbor.

Off: SIP INVITEs will be generated and a pre-configured SDP will be inserted before the INVITEs are sent to this neighbor.

Default: On

Example: `xConfiguration Zones Zone 1 DNS Interworking SIP EmptyInviteAllowed: On`

Zones Zone [1..1000] DNS Interworking SIP Video DefaultBitrate: <64..65535>

Specifies which video bitrate to use when empty INVITEs are not allowed.

Default: 384

Example: `xConfiguration Zones Zone 1 DNS Interworking SIP Video DefaultBitrate: 384`

Zones Zone [1..1000] DNS Interworking SIP Video DefaultCodec: <None/H261/H263/H263p/H263pp/H264>

Specifies which video codec to use when empty INVITEs are not allowed.

Default: H263

Example: `xConfiguration Zones Zone 1 DNS Interworking SIP Video DefaultCodec: H263`

Zones Zone [1..1000] DNS Interworking SIP Video DefaultResolution: <None/QCIF/CIF/4CIF/SIF/4SIF/VGA/SVGA/XGA>

Specifies which video resolution to use when empty INVITEs are not allowed.

Default: CIF

Example: `xConfiguration Zones Zone 1 DNS Interworking SIP Video DefaultResolution: CIF`

Zones Zone [1..1000] DNS SIP Duo Video Filter Mode: <On/Off>

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.

On: the second video line in any outgoing INVITE request is removed.

Off: INVITE requests are not modified.

Default: Off

Example: `xConfiguration Zones Zone 1 DNS SIP Duo Video Filter Mode: Off`

Zones Zone [1..1000] DNS SIP Poison Mode: <On/Off>

Determines whether SIP requests sent out to this zone will be "poisoned" such that if they are received by the local VCS again they will be rejected.

On: SIP requests sent out via this zone that are received again by this VCS will be rejected.

Off: SIP requests sent out via this zone that are received by this VCS again will be processed as normal.

Default: Off

Example: **xConfiguration Zones Zone 1 DNS SIP Poison Mode: Off**

Zones Zone [1..1000] DNS SIP Record Route Address Type: <IP/Hostname>

Controls whether the VCS uses its IP address or host name in the record-route or path headers of outgoing SIP requests to this zone.

Note: setting this value to Hostname also requires a valid DNS local host name to be configured on the VCS.

Default: IP

Example: **xConfiguration Zones Zone [1..1000] DNS SIP Record Route Address Type: IP**

Zones Zone [1..1000] DNS SIP SDP Attribute Line Limit Length: <80..65535>

If SIP SDP attribute line limit mode is set to On, sets the maximum line length of a=fmtp SDP lines.

Default: 130

Example: **xConfiguration Zones Zone 1 DNS SIP SDP Attribute Line Limit Length: 130**

Zones Zone [1..1000] DNS SIP SDP Attribute Line Limit Mode: <On/Off>

Determines whether requests containing SDP sent out to this zone will have the length of a=fmtp lines restricted.

On: the length will be truncated to the maximum length specified by the SIP SDP attribute line limit length setting.

Off: the length will not be truncated.

Example: **xConfiguration Zones Zone 1 DNS SIP SDP Attribute Line Limit Mode: Off**

Zones Zone [1..1000] DNS SIP SearchAutoResponse: <On/Off>

Determines what happens when the VCS receives a SIP search that originated as an H.323 search, destined for this zone.

Off: a SIP OPTION message will be sent to the zone.

On: searches will be responded to automatically, without being forwarded to the zone.

Default: Off

Example: **xConfiguration Zones Zone 1 DNS SIP SearchAutoResponse: Off**

Zones Zone [1..1000] DNS SIP TLS Verify Mode: <On/Off>

Controls X.509 certificate checking between this VCS and the destination system server returned by the DNS lookup. When enabled, the domain name submitted to the DNS lookup must be contained within the server's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes).

Default: Off

Example: **xConfiguration Zones Zone 1 DNS SIP TLS Verify Mode: On**

Zones Zone [1..1000] DNS SIP UDP BFCP Filter Mode: <On/Off>

Determines whether INVITE requests sent to this zone filter out UDP/BFCP. This option may be required to enable interoperability with SIP devices that do not support the UDP/BFCP protocol.

On: any media line referring to the UDP/BFCP protocol is replaced with TCP/BFCP and disabled.

Off: INVITE requests are not modified.

Default: Off

Example: `xConfiguration Zones Zone 1 DNS SIP UDP BFCP Filter Mode: Off`

Zones Zone [1..1000] DNS ZoneProfile: <Default/Custom/MicrosoftOCS2007/ CiscoUnifiedCommunicationsManager/NortelCS1000/AdvancedMediaGateway/NonRegisteringDevice>

Determines the way in which the advanced settings for this zone are configured.

Default: uses the factory defaults for these settings.

Custom: allows you to configure each setting individually.

Preconfigured profiles: alternatively, choose one of the preconfigured profiles to automatically use the appropriate settings required for connections to that type of system.

Default: Default

Example: `xConfiguration Zones Zone 1 DNS ZoneProfile: Default`

Zones Zone [1..1000] ENUM DNSSuffix: <S: 0, 128>

Specifies the DNS zone to be appended to the transformed E.164 number to create an ENUM host name which this zone is then queried for.

Example: `xConfiguration Zones Zone 2 ENUM DNSSuffix: "e164.arpa"`

Zones Zone [1..1000] H323 Mode: <On/Off>

Determines whether H.323 calls will be allowed to and from this zone.

Default: On

Example: `xConfiguration Zones Zone 2 H323 Mode: On`

Zones Zone [1..1000] HopCount: <1..255>

Specifies the hop count to be used when sending an alias search request to this zone. Note: if the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used.

Default: 15

Example: `xConfiguration Zones Zone 2 HopCount: 15`

Zones Zone [1..1000] Name: <S: 1, 50>

Assigns a name to this zone.

Example: `xConfiguration Zones Zone 3 Name: "UK Sales Office"`

Zones Zone [1..1000] Neighbor AdvancedMediaGateway Mode: <On/Off>

Controls whether calls to or from this zone will use an Advanced Media Gateway.

Default: Off

Example: `xConfiguration Zones Zone 3 Neighbor AdvancedMediaGateway Mode: On`

Zones Zone [1..1000] Neighbor Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

Controls how the VCS authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. See the Administrator Guide for full details about each of the Authentication Policy options.

Default: DoNotCheckCredentials

Example: **`xConfiguration Zones Zone 1 Neighbor Authentication Mode: DoNotCheckCredentials`**

Zones Zone [1..1000] Neighbor H323 Port: <1024..65534>

Specifies the port on the neighbor to be used for H.323 calls to and from this VCS.

Default: 1719

Example: **`xConfiguration Zones Zone 3 Neighbor H323 Port: 1719`**

Zones Zone [1..1000] Neighbor H323 SearchAutoResponse: <On/Off>

Determines what happens when the VCS receives a H323 search, destined for this zone.

Off: an LRQ message will be sent to the zone.

On: searches will be responded to automatically, without being forwarded to the zone.

Default: Off

Example: **`xConfiguration Zones Zone 1 Neighbor H323 SearchAutoResponse: Off`**

Zones Zone [1..1000] Neighbor Interworking SIP Audio DefaultCodec: <G711u/G711a/G722_48/G722_56/G722_64/G722_1_16/G722_1_24/G722_1_32/G722_1_48/G723_1/G728/G729/AALCD_48/AALCD_56/AALCD_64/AMR>

Specifies which audio codec to use when empty INVITEs are not allowed.

Default: G711u

Example: **`xConfiguration Zones Zone 3 Neighbor Interworking SIP Audio DefaultCodec: G711u`**

Zones Zone [1..1000] Neighbor Interworking SIP EmptyInviteAllowed: <On/Off>

Determines whether the VCS will generate a SIP INVITE message with no SDP to send to this zone. INVITEs with no SDP mean that the destination device is asked to initiate the codec selection, and are used when the call has been interworked locally from H.323.

On: SIP INVITEs with no SDP will be generated and sent to this neighbor.

Off: SIP INVITEs will be generated and a pre-configured SDP will be inserted before the INVITEs are sent to this neighbor.

Default: On

Example: **`xConfiguration Zones Zone 3 Neighbor Interworking SIP EmptyInviteAllowed: On`**

Zones Zone [1..1000] Neighbor Interworking SIP Search Strategy: <Options/Info>

Determines how the VCS will search for SIP endpoints when interworking an H.323 call.

Options: the VCS will send an OPTIONS request.

Info: the VCS will send an INFO request.

Default: Options

Example: **`xConfiguration Zones Zone 3 Neighbor Interworking SIP Search Strategy: Options`**

Zones Zone [1..1000] Neighbor Interworking SIP Video DefaultBitrate: <64..65535>

Specifies which video bitrate to use when empty INVITEs are not allowed.

Default: 384

Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP Video DefaultBitrate: 384`

Zones Zone [1..1000] Neighbor Interworking SIP Video DefaultCodec: <None/H261/H263/H263p/H263pp/H264>

Specifies which video codec to use when empty INVITEs are not allowed.

Default: H263

Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP Video DefaultCodec: H263`

Zones Zone [1..1000] Neighbor Interworking SIP Video DefaultResolution: <None/QCIF/CIF/4CIF/SIF/4SIF/VGA/SVGA/XGA>

Specifies which video resolution to use when empty INVITEs are not allowed.

Default: CIF

Example: `xConfiguration Zones Zone 3 Neighbor Interworking SIP Video DefaultResolution: CIF`

Zones Zone [1..1000] Neighbor Monitor: <Yes/No>

Specifies whether the zone monitors the aliveness of its neighbor peers. H323 LRQs and/or SIP OPTIONS will be periodically sent to the peers. If any peer fails to respond, that peer will be marked as inactive. If no peer manages to respond the zone will be marked as inactive.

Default: Yes

Example: `xConfiguration Zones Zone 1 Neighbor Monitor: Yes`

Zones Zone [1..1000] Neighbor Peer [1..6] Address: <S:0,128>

Specifies the IP address or Fully Qualified Domain Name (FQDN) of the neighbor. If the neighbor zone is a VCS cluster, this will be one of the peers in that cluster.

Example: `xConfiguration Zones Zone 3 Neighbor Peer 1 Address: "192.44.0.18"`

Zones Zone [1..1000] Neighbor Registrations: <Allow/Deny>

Controls whether proxied SIP registrations routed through this zone are accepted.

Default: Allow

Example: `xConfiguration Zones Zone 3 Neighbor Registrations: Allow`

Zones Zone [1..1000] Neighbor SIP Authentication Trust Mode: <On/Off>

Controls whether authenticated SIP messages (ones containing a P-Asserted-Identity header) from this zone are trusted.

On: messages are trusted without further challenge.

Off: messages are challenged for authentication.

Default: Off

Example: `xConfiguration Zones Zone 3 Neighbor SIP Authentication Trust Mode: On`

Zones Zone [1..1000] Neighbor SIP Duo Video Filter Mode: <On/Off>

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.

On: the second video line in any outgoing INVITE request is removed.

Off: INVITE requests are not modified.

Default: Off

Example: `xConfiguration Zones Zone 1 Neighbor SIP Duo Video Filter Mode: Off`

Zones Zone [1..1000] Neighbor SIP Encryption Mode: <Auto/Microsoft/Off>

Determines how the VCS handles 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.

Default: Auto

Example: `xConfiguration Zones Zone 3 Neighbor SIP Encryption Mode: Auto`

Zones Zone [1..1000] Neighbor SIP MIME Strip Mode: <On/Off>

Controls whether multipart MIME stripping is performed on requests from this zone. This must be set to On for connections to a Microsoft Office Communications Server 2007.

Default: Off

Example: `xConfiguration Zones Zone 3 Neighbor SIP MIME Strip Mode: Off`

Zones Zone [1..1000] Neighbor SIP MediaRouting Mode: <Auto/Signaled/Latching>

Specifies how the VCS handles the media for calls to and from this neighbor, and where it will forward the media destined for this neighbor.

Signaled: the media is always taken for calls to and from this neighbor. It will be forwarded as signaled in the SDP received from this neighbor.

Latching: the media is always taken for calls to and from this neighbor. It will be forwarded to the IP address and port from which media from this neighbor is received.

Auto: media is only taken if the call is a traversal call. If this neighbor is behind a NAT the VCS will forward the media to the IP address and port from which media from this zone is received (latching). Otherwise it will forward the media to the IP address and port signaled in the SDP (signaled).

Default: Auto.

Example: `xConfiguration Zones Zone 3 Neighbor SIP MediaRouting Mode: Auto`

Zones Zone [1..1000] Neighbor SIP Poison Mode: <On/Off>

Determines whether SIP requests sent out to this zone will be "poisoned" such that if they are received by the local VCS again they will be rejected.

On: SIP requests sent out via this zone that are received again by this VCS will be rejected.

Off: SIP requests sent out via this zone that are received by this VCS again will be processed as normal.

Default: Off

Example: `xConfiguration Zones Zone 3 Neighbor SIP Poison Mode: Off`

Zones Zone [1..1000] Neighbor SIP Port: <1024..65534>

Specifies the port on the neighbor to be used for SIP calls to and from this VCS.

Default: 5061

Example: **xConfiguration Zones Zone 3 Neighbor SIP Port: 5061**

Zones Zone [1..1000] Neighbor SIP ProxyRequire Strip List: <S: 0,255>

A comma separated list of option tags to search for and remove from Proxy-Require headers in SIP requests received from this zone. By default, no option tags are specified.

Example: **xConfiguration Zones Zone 3 Neighbor SIP ProxyRequire Strip List: "com.example.something,com.example.somethingelse"**

Zones Zone [1..1000] Neighbor SIP Record Route Address Type: <IP/Hostname>

Controls whether the VCS uses its IP address or host name in the record-route or path headers of outgoing SIP requests to this zone.

Note: setting this value to Hostname also requires a valid DNS local host name to be configured on the VCS.

Default: IP

Example: **xConfiguration Zones Zone [1..1000] Neighbor SIP Record Route Address Type: IP**

Zones Zone [1..1000] Neighbor SIP SDP Attribute Line Limit Length: <80..65535>

If SIP SDP attribute line limit mode is set to On, sets the maximum line length of a=fmtp SDP lines.

Default: 130

Example: **xConfiguration Zones Zone 3 Neighbor SIP SDP Attribute Line Limit Length: 130**

Zones Zone [1..1000] Neighbor SIP SDP Attribute Line Limit Mode: <On/Off>

Determines whether requests containing SDP sent out to this zone will have the length of a=fmtp lines restricted.

On: the length will be truncated to the maximum length specified by the SIP SDP attribute line limit length setting.

Off: the length will not be truncated.

Default: Off

Example: **xConfiguration Zones Zone 3 Neighbor SIP SDP Attribute Line Limit Mode: Off**

Zones Zone [1..1000] Neighbor SIP SearchAutoResponse: <On/Off>

Determines what happens when the VCS receives a SIP search that originated as an H.323 search, destined for this zone.

Off: a SIP OPTION message will be sent to the zone.

On: searches will be responded to automatically, without being forwarded to the zone.

Default: Off

Example: **xConfiguration Zones Zone 3 Neighbor SIP SearchAutoResponse: Off**

Zones Zone [1..1000] Neighbor SIP TLS Verify Mode: <On/Off>

Controls X.509 certificate checking and mutual authentication for inbound and outbound connections between this VCS and the neighbor system. When enabled, the neighbor system's FQDN or IP address, as specified in the Peer address field, must be contained within the neighbor's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes).

Default: Off

Example: `xConfiguration Zones Zone 3 Neighbor SIP TLS Verify Mode: On`

Zones Zone [1..1000] Neighbor SIP Transport: <UDP/TCP/TLS>

Determines which transport type will be used for SIP calls to and from this neighbor.

Default: TLS

Example: `xConfiguration Zones Zone 3 Neighbor SIP Transport: TLS`

Zones Zone [1..1000] Neighbor SIP UDP BFCP Filter Mode: <On/Off>

Determines whether INVITE requests sent to this zone filter out UDP/BFCP. This option may be required to enable interoperability with SIP devices that do not support the UDP/BFCP protocol.

On: any media line referring to the UDP/BFCP protocol is replaced with TCP/BFCP and disabled.

Off: INVITE requests are not modified.

Default: Off

Example: `xConfiguration Zones Zone 1 Neighbor SIP UDP BFCP Filter Mode: Off`

Zones Zone [1..1000] Neighbor SIP UPDATE Strip Mode: <On/Off>

Determines whether or not the VCS will strip the UPDATE method from the Allow header of all requests and responses going to and from this zone.

Default: Off

Example: `xConfiguration Zones Zone 3 Neighbor SIP UPDATE Strip Mode: Off`

Zones Zone [1..1000] Neighbor ZoneProfile: <Default/Custom/MicrosoftOCS2007/ CiscoUnifiedCommunicationsManager/NortelCS1000/AdvancedMediaGateway/NonRegisteringDevice>

Determines the way in which the advanced settings for this zone are configured.

Default: uses the factory defaults for thesesettings.

Custom: allows you to configure each setting individually.

Preconfigured profiles: alternatively, choose one of the preconfigured profiles to automatically use the appropriate settings required for connections to that type of system.

Default: Default

Example: `Zones Zone 3 Neighbor ZoneProfile: Default`

Zones Zone [1..1000] SIP Mode: <On/Off>

Determines whether SIP calls will be allowed to and from this zone.

Default: On

Example: `xConfiguration Zones Zone 3 SIP Mode: On`

Zones Zone [1..1000] TraversalClient Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

Controls how the VCS authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. See the Administrator Guide for full details about each of the Authentication Policy options.

Default: DoNotCheckCredentials

Example: `xConfiguration Zones Zone [1..1000] TraversalClient Authentication Mode: DoNotCheckCredentials`

Zones Zone [1..1000] TraversalClient Authentication Password: <S: 0,215>

The password used by the VCS when connecting to the traversal server. The maximum plaintext length is 128 characters, which is then encrypted.

Example: `xConfiguration Zones Zone 1 TraversalClient Authentication Password: "password123"`

Zones Zone [1..1000] TraversalClient Authentication UserName: <S: 0,128>

The user name used by the VCS when connecting to the traversal server.

Example: `xConfiguration Zones Zone 1 TraversalClient Authentication UserName: "clientname"`

Zones Zone [1..1000] TraversalClient H323 Port: <1024..65534>

Specifies the port on the traversal server to be used for H.323 firewall traversal calls from this VCS. If the traversal server is a VCS Expressway, this must be the port number that has been configured on the VCS Expressway's traversal server zone associated with this VCS.

Example: `xConfiguration Zones Zone 4 TraversalClient H323 Port: 2777`

Zones Zone [1..1000] TraversalClient H323 Protocol: <Assent/H46018>

Determines which of the two firewall traversal protocols will be used for calls to and from the traversal server.

Note: the same protocol must be set on the server for calls to and from this traversal client.

Default: Assent

Example: `xConfiguration Zones Zone 4 TraversalClient H323 Protocol: Assent`

Zones Zone [1..1000] TraversalClient Peer [1..6] Address: <S:0,128>

Specifies the IP address or Fully Qualified Domain Name (FQDN) of the traversal server. If the traversal server is a VCS Expressway cluster, this will be one of the peers in that cluster.

Example: `xConfiguration Zones Zone 4 TraversalClient Peer 1 Address: "10.192.168.1"`

Zones Zone [1..1000] TraversalClient Registrations: <Allow/Deny>

Controls whether proxied SIP registrations routed through this zone are accepted.

Default: Allow

Example: `xConfiguration Zones Zone 4 TraversalClient Registrations: Allow`

Zones Zone [1..1000] TraversalClient RetryInterval: <1..65534>

Specifies the interval (in seconds) with which a failed attempt to establish a connection to the traversal server should be retried.

Default: 120

Example: `xConfiguration Zones Zone 4 TraversalClient RetryInterval: 120`

Zones Zone [1..1000] TraversalClient SIP Poison Mode: <On/Off>

Determines whether SIP requests sent out to this zone will be "poisoned" such that if they are received by the local VCS again they will be rejected.

On: SIP requests sent out via this zone that are received again by this VCS will be rejected.

Off: SIP requests sent out via this zone that are received by this VCS again will be processed as normal.

Default: Off

Example: **xConfiguration Zones Zone 4 TraversalClient SIP Poison Mode: Off**

Zones Zone [1..1000] TraversalClient SIP Port: <1024..65534>

Specifies the port on the traversal server to be used for SIP calls from this VCS. If your traversal server is a VCS Expressway, this must be the port number that has been configured in the traversal server zone for this VCS.

Example: **xConfiguration Zones Zone 4 TraversalClient SIP Port: 5061**

Zones Zone [1..1000] TraversalClient SIP Protocol: <Assent/TURN/ICE>

Determines which firewall traversal protocol will be used for SIP calls to and from the traversal server. Note: the same protocol must be set on the server for calls to and from this traversal client.

Default: Assent

Example: **xConfiguration Zones Zone 1 TraversalClient SIP Protocol: Assent**

Zones Zone [1..1000] TraversalClient SIP TLS Verify Mode: <On/Off>

Controls X.509 certificate checking and mutual authentication between this VCS and the traversal server. When enabled, the server's FQDN or IP address, as specified in the Peer address field, must be contained within the server's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes).

Default: Off

Example: **xConfiguration Zones Zone 4 TraversalClient SIP TLS Verify Mode: On**

Zones Zone [1..1000] TraversalClient SIP Transport: <TCP/TLS>

Determines which transport type will be used for SIP calls to and from the traversal server.

Default: TLS

Example: **xConfiguration Zones Zone 4 TraversalClient SIP Transport: TLS**

Zones Zone [1..1000] TraversalServer Authentication Mode: <DoNotCheckCredentials/TreatAsAuthenticated/CheckCredentials>

Controls how the VCS authenticates incoming messages from this zone and whether they are subsequently treated as authenticated, unauthenticated, or are rejected. The behavior varies for H.323 messages, SIP messages that originate from a local domain and SIP messages that originate from non-local domains. See the online help for full details about each of the Authentication Policy options.

Default: DoNotCheckCredentials

Example: **xConfiguration Zones Zone 1 TraversalServer Authentication Mode: DoNotCheckCredentials**

Zones Zone [1..1000] TraversalServer Authentication UserName: <S: 0,128>

The name used by the traversal client when authenticating with the traversal server. If the traversal client is a VCS, this must be the VCS's authentication user name. If the traversal client is a gatekeeper, this must be the gatekeeper's System Name. For other types of traversal clients, refer to the VCS Admin Guide for further information.

Example: **xConfiguration Zones Zone 5 TraversalServer Authentication UserName: "User123"**

Zones Zone [1..1000] TraversalServer H323 H46019 Demultiplexing Mode: <On/Off>

Determines whether the VCS will operate in demultiplexing mode for calls from the traversal client.

On: allows use of the same two ports for all calls.

Off: each call will use a separate pair of ports for media.

Default: Off

Example: **xConfiguration Zones Zone 5 TraversalServer H323 H46019 Demultiplexing Mode: Off**

Zones Zone [1..1000] TraversalServer H323 Port: <1024..65534>

Specifies the port on the VCS being used for H.323 firewall traversal from this traversal client.

Default: 6001, incrementing by 1 for each new zone.

Example: **xConfiguration Zones Zone 5 TraversalServer H323 Port: 2777**

Zones Zone [1..1000] TraversalServer H323 Protocol: <Assent/H46018>

Determines which of the two firewall traversal protocols will be used for calls to and from the traversal client.

Note: the same protocol must be set on the client for calls to and from this traversal server.

Default: Assent

Example: **xConfiguration Zones Zone 5 TraversalServer H323 Protocol: Assent**

Zones Zone [1..1000] TraversalServer Registrations: <Allow/Deny>

Controls whether proxied SIP registrations routed through this zone are accepted.

Default: Allow

Example: **xConfiguration Zones Zone 5 TraversalServer Registrations: Allow**

Zones Zone [1..1000] TraversalServer SIP Poison Mode: <On/Off>

Determines whether SIP requests sent out to this zone will be "poisoned" such that if they are received by the local VCS again they will be rejected.

On: SIP requests sent out via this zone that are received again by this VCS will be rejected.

Off: SIP requests sent out via this zone that are received by this VCS again will be processed as normal.

Default: Off

Example: **xConfiguration Zones Zone 5 TraversalServer SIP Poison Mode: Off**

Zones Zone [1..1000] TraversalServer SIP Port: <1024..65534>

Specifies the port on the VCS being used for SIP firewall traversal from this traversal client.

Default: 7001, incrementing by 1 for each new zone.

Example: **xConfiguration Zones Zone 5 TraversalServer SIP Port: 5061**

Zones Zone [1..1000] TraversalServer SIP Protocol: <Assent/TURN/ICE>

Determines which firewall traversal protocol will be used for SIP calls to and from the traversal client. Note: the same protocol must be set on the client for calls to and from this traversal server.

Default: Assent

Example: `xConfiguration Zones Zone 1 TraversalServer SIP Protocol: Assent`

Zones Zone [1..1000] TraversalServer SIP TLS Verify Mode: <On/Off>

Controls X.509 certificate checking and mutual authentication between this VCS and the traversal client. If enabled, a TLS verify subject name must be specified.

Default: Off

Example: `xConfiguration Zones Zone 5 TraversalServer SIP TLS Verify Mode: On`

Zones Zone [1..1000] TraversalServer SIP TLS Verify Subject Name: <S: 0,128>

The certificate holder's name to look for in the traversal client's X.509 certificate (must be in either the Subject Common Name or the Subject Alternative Name attributes).

Example: `xConfiguration Zones Zone 5 TraversalServer SIP TLS Verify Subject Name: "myclientname"`

Zones Zone [1..1000] TraversalServer SIP Transport: <TCP/TLS>

Determines which of the two transport types will be used for SIP calls between the traversal client and VCS.

Default: TLS

Example: `xConfiguration Zones Zone 5 TraversalServer SIP Transport: TLS`

Zones Zone [1..1000] TraversalServer TCPProbe KeepAliveInterval: <1..65534>

Sets the interval (in seconds) with which the traversal client will send a TCP probe to the VCS once a call is established, in order to keep the firewall's NAT bindings open.

Default: 20

Example: `xConfiguration Zones Zone 5 TraversalServer TCPProbe KeepAliveInterval: 20`

Zones Zone [1..1000] TraversalServer TCPProbe RetryCount: <1..65534>

Sets the number of times the traversal client will attempt to send a TCP probe to the VCS.

Default: 5

Example: `xConfiguration Zones Zone 5 TraversalServer TCPProbe RetryCount: 5`

Zones Zone [1..1000] TraversalServer TCPProbe RetryInterval: <1..65534>

Sets the frequency (in seconds) with which the traversal client will send a TCP probe to the VCS.

Default: 2

Example: `xConfiguration Zones Zone 5 TraversalServer TCPProbe RetryInterval: 2`

Zones Zone [1..1000] TraversalServer UDPProbe KeepAliveInterval: <1..65534>

Sets the interval (in seconds) with which the traversal client will send a UDP probe to the VCS once a call is established, in order to keep the firewall's NAT bindings open.

Default: 20

Example: `xConfiguration Zones Zone 5 TraversalServer UDPProbe KeepAliveInterval: 20`

Zones Zone [1..1000] TraversalServer UDPProbe RetryCount: <1..65534>

Sets the number of times the traversal client will attempt to send a UDP probe to the VCS.

Default: 5

Example: `xConfiguration Zones Zone 5 TraversalServer UDPProbe RetryCount: 5`

Zones Zone [1..1000] TraversalServer UDPProbe RetryInterval: <1..65534>

Sets the frequency (in seconds) with which the traversal client will send a UDP probe to the VCS.

Default: 2

Example: `xConfiguration Zones Zone 5 TraversalServer UDPProbe RetryInterval: 2`

Zones Zone [1..1000] Type: <Neighbor/TraversalClient/TraversalServer/ENUM/DNS>

Determines the nature of the specified zone, in relation to the local VCS.

Neighbor: the new zone will be a neighbor of the local VCS.

TraversalClient: there is a firewall between the zones, and the local VCS is a traversal client of the new zone.

TraversalServer: there is a firewall between the zones and the local VCS is a traversal server for the new zone.

ENUM: the new zone contains endpoints discoverable by ENUM lookup.

DNS: the new zone contains endpoints discoverable by DNS lookup.

Example: `xConfiguration Zones Zone 3 Type: Neighbor`

xCommand command reference

The **xCommand** group of commands are used to add and delete items and issue system commands.

The following section lists all the currently available **xCommand** commands.

To issue a command, type the command as shown, followed by one or more of the given parameters and values. The valid values for each parameter are indicated in the angle brackets following each parameter, using the following notation:

Format	Meaning
<0..63>	Indicates an integer value is required. The numbers indicate the minimum and maximum value. In this example the value must be in the range 0 to 63.
<S: 7,15>	An **S** indicates a string value, to be enclosed in quotation marks, is required. The numbers indicate the minimum and maximum number of characters for the string. In this example the string must be between 7 and 15 characters long.
<Off/Direct/Indirect>	Lists the set of valid values for the command. Do not enclose the value in quotation marks
(r)	(r) indicates that this is a required parameter. Note that the (r) is not part of the command itself.

To obtain information about using each of the **xCommand** commands from within the CLI, type:

- **xCommand** or **xCommand ?** to return a list of all available **xCommand**commands.
- **xCommand ??** to return all current **xCommand**commands, along with a description of each command, a list of its parameters, and for each parameter its valuespaces and description.
- **xCommand <command> ?** to return a description of the command, a list of its parameters, and for each parameter its valuespaces and description.

xCommand commands

All of the available **xCommand** commands are listed in the table below:

AMGWPolicyRuleAdd

Adds and configures a new Advanced Media Gateway policy rule.

Name(r): <S: 1,50>

Assigns a name to this Advanced Media Gateway policy rule.

Description: <S: 0,64>

A free-form description of the membership rule.

Example: **xCommand AMGWPolicyRuleAdd Name: "Deny branch calls" Description: "Deny all calls to branch office"**

AMGWPolicyRuleDelete

Deletes an Advanced Media Gateway policy rule.

AMGWPolicyRuleId(r): <1..200>

The index of the Advanced Media Gateway policy rule to be deleted.

Example: **xCommand AMGWPolicyRuleDelete AMGWPolicyRuleId: 1**

AdminAccountAdd

Creates a new administrator account.

Name(r): <S:0,25>

Defines the name of an administrator user who can login to the VCS web interface.

Password(r): <S:0,65>

Defines the password of an administrator user who can login to the VCS web interface. The maximum plaintext length is 16 characters, which will then be encrypted.

Access(r): <AccountDisabled/ReadOnly/ReadWrite/Auditor>

Defines the access level of an administrator user who can login to the VCS web interface. *AccountDisabled*: no access allowed. *ReadOnly*: configuration can only be viewed. *ReadWrite*: configuration can be viewed and changed. *Auditor*: allows access to the Event Log, Configuration Log and the Overview page only.
Default: ReadWrite

Example: **xCommand AdminAccountAdd Name: "guest" Password: "password123" Access: readonly**

AdminAccountDelete

Deletes an administrator account.

AdminAccountId(r): <1..15>

The index of the administrator account to be deleted.

Example: **xCommand AdminAccountDelete AdminAccountId: 1**

AdminLoginGroupAdd

Creates a new administrator login group.

Name(r): <S: 0,128>

Defines the name of an administrator group that determines which access rights members of the group have after they have been successfully authenticated to use the VCS.

Access(r): <None/ReadOnly/ReadWrite/Auditor>

Defines the access level for members of the specified administrator group. *None*: no access allowed. *ReadOnly*: configuration can only be viewed. *ReadWrite*: configuration can be viewed and changed. *Auditor*: allows access to the Event Log, Configuration Log and the Overview page only.
Default: ReadWrite

Example: **xCommand AdminLoginGroupAdd Name: "VCS" Access: ReadWrite**

AdminLoginGroupDelete

Deletes an administrator login group.

AdminLoginGroupId(r): <1..30>

The index of the administrator login group to be deleted.

Example: **xCommand AdminLoginGroupDelete AdminLoginGroupId: 1**

AdsDcAdd

Adds a new Active Directory server.

ActiveDirectoryAddress(r): <S: 0,39>

The address of a domain controller that can be used when the VCS joins the AD domain. Not specifying a specific AD will result the use of DNS SRV queries to find an AD.

Example: **xCommand AdsDcAdd ActiveDirectoryAddress: "192.168.0.0"**

AdsDcDelete

Deletes an Active Directory server.

ActiveDirectoryId(r): <1..5>

The index of the Active Directory server to be deleted.

Example: **xCommand AdsDcDelete ActiveDirectoryId: 1**

AdsKdcAdd

Adds a new Kerberos KDC.

KerberosKDCAddress(r): <S: 0,39>

The address of a Kerberos Distribution Center (KDC) to be used when connected to the AD domain. Not specifying a specific KDC will result in the use of DNS SRV queries to find a KDC.

KerberosKDCPort: <1..65534>

Specifies the port of a KDC that can be used when the VCS joins the AD domain. Default: 88

Example: **xCommand AdsKdcAdd KerberosKDCAddress: "192.168.0.0" KerberosKDCPort: 88**

AdsKdcDelete

Deletes a configured Kerberos KDC.

KerberosKDCId(r): <1..5>

The index of the Kerberos KDC to be deleted.

Example: **xCommand AdsKdcDelete KerberosKDCId: 1**

AllowListAdd

Adds an entry to the Allow List.

PatternString(r): <S: 1, 60>

Specifies an entry to be added to the Allow List. If one of an endpoint's aliases matches one of the patterns in the Allow List, the registration will be permitted.

PatternType: <Exact/Prefix/Suffix/Regex>

Specifies whether the entry in the Allow List is a prefix, suffix, regular expression, or must be matched exactly. *Exact*: the string must match the alias character for character. *Prefix*: the string must appear at the beginning of the alias. *Suffix*: the string must appear at the end of the alias. *Regex*: the string will be treated as a regular expression.
Default: Exact.

Description: <S: 0,64>

A free-form description of the Allow List rule.

Example: **xCommand AllowListAdd PatternString: "John.Smith@example.com" PatternType: Exact Description: "Allow John Smith"**

AllowListDelete

Deletes an entry from the Allow List.

AllowListId(r): <1..2500>

The index of the entry to be deleted.

Example: **xCommand AllowListDelete AllowListId: 2**

Boot

Reboots the VCS.

This command has no parameters.

Example: **xCommand boot**

CheckBandwidth

A diagnostic tool that returns the status and route (as a list of nodes and links) that a call of the specified type and bandwidth would take between two nodes. Note that this command does not change any existing system configuration.

Node1(r): <S: 1, 50>

The subzone or zone from which the call originates.

Node2(r): <S: 1, 50>

The subzone or zone at which the call terminates.

Bandwidth(r): <1..100000000>

The requested bandwidth of the call (in kbps).

CallType(r): <Traversal/NonTraversal>

Whether the call type is Traversal or Non-traversal.

Example: **xCommand CheckBandwidth Node1: "DefaultSubzone" Node2: "UK Sales Office" Bandwidth: 512 CallType: nontraversal**

CheckPattern

A diagnostic tool that allows you to check the result of an alias transform (local or zone) before you configure it on the system. Note that this command does not change any existing system configuration.

Target(r): <S: 1, 60>

The alias you want to use to test the pattern match or transform.

Pattern(r): <S: 1, 60>

The pattern against which the alias is compared.

Type(r): <Exact/Prefix/Suffix/Regex>

How the pattern string must match the alias for the pattern behavior to be applied.

Behavior(r): <Strip/Leave/Replace/AddPrefix/AddSuffix>

How the alias is modified.

Replace: <S: 0, 60>

The text string to use in conjunction with the selected Pattern behavior.

Example: **xCommand CheckPattern Target: "john.smith@example.net" Pattern: "@example.net" Type: "suffix" Behavior: replace Replace: "@example.com"**

CredentialAdd

Adds an entry to the local authentication database.

CredentialName(r): <S: 1, 128>

Defines the name for this entry in the local authentication database.

CredentialPassword(r): <S: 1, 128>

Defines the password for this entry in the local authentication database.

Example: **xCommand CredentialAdd CredentialName: "John Smith" CredentialPassword: "password123"**

CredentialDelete

Deletes an entry from the local authentication database.

CredentialId(r): <1..2500>

The index of the credential to be deleted.

Example: **xCommand CredentialDelete CredentialId: 2**

DefaultLinksAdd

Restores links between the Default Subzone, Traversal Subzone and the Default Zone.

This command has no parameters.

Example: **xCommand DefaultLinksAdd**

DefaultValuesSet

Resets system parameters to default values.

Level(r): <1..3>

The level of system parameters to be reset.
Level 1: resets most configuration items to their default value, with the exception of the Level 2 and Level 3 items.
Level 2: resets configuration items related to remote authentication, plus Level 1 items to their default value.
Level 3: resets all critical configuration items, plus Level 1 and Level 2 items to their default value. See the Restoring default configuration section for full details.

Example: **xCommand DefaultValuesSet Level: 1**

DenyListAdd

Adds an entry to the Deny List.

PatternString(r): <S: 1, 60>

Specifies an entry to be added to the Deny List. If one of an endpoint's aliases matches one of the patterns in the Deny List, the registration will not be permitted.

PatternType: <Exact/Prefix/Suffix/Regex>

Specifies whether the entry in the Deny List is a prefix, suffix, regular expression, or must be matched exactly. *Exact*: the string must match the alias character for character. *Prefix*: the string must appear at the beginning of the alias. Suffix: the string must appear at the end of the alias. *Regex*: the string will be treated as a regular expression.
Default: Exact.

Description: <S: 0, 64>

A free-form description of the Deny List rule.

Example: **xCommand DenyListAdd PatternString: "sally.jones@example.com" PatternType: exact Description: "Deny Sally Jones"**

DenyListDelete

Deletes an entry from the Deny List.

DenyListId(r): <1..2500>

The index of the entry to be deleted.

Example: **xCommand DenyListDelete DenyListId: 2**

DisconnectCall

Disconnects a call.

Call: <1..900>

The index of the call to be disconnected.

CallSerialNumber: <S: 1, 255>

The serial number of the call to be disconnected. Note: you must specify either a call index or call serial number when using this command.

Example: **xCommand DisconnectCall CallSerialNumber: "6d843434-211c-11b2-b35d-0010f30f521c"**

DomainAdd

Adds a SIP domain for which this VCS is authoritative.

DomainName(r): <S: 1, 128>

Specifies a domain for which this VCS is authoritative. The VCS will act as a SIP registrar and Presence Server for this domain, and will accept registration requests for any SIP endpoints attempting to register with an alias that includes this domain. 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.

Example: **xCommand DomainAdd DomainName: "100.example-name.com"**

DomainDelete

Deletes a domain.

DomainId(r): <1..20>

The index of the domain to be deleted.

Example: **xCommand DomainDelete DomainId: 2**

ExtAppStatusAdd

Allows another application running on the VCS to attach xstatus to the VCS XML xstatus tree.

Note: this command is intended for developer use only.

Name(r): <S:1, 64>

Descriptive name for the external application whose status is being referenced.

Filename(r): <S:0, 255>

XML file containing status that is to be attached for an external application.

Example: **xCommand ExtAppStatusAdd Name: "foo" Filename: "foo.xml"**

ExtAppStatusDelete

Deletes an external application status entry.

Note: this command is intended for developer use only.

Name(r): <S:1, 64>

Descriptive name for the external application whose status is being referenced.

Example: **xCommand ExtAppStatusDelete Name: foo**

FeedbackDeregister

Deactivates a particular feedback request.

ID: <1..3>

The index of the feedback request to be deactivated.

Example: **xCommand FeedbackDeregister ID: 1**

FeedbackRegister

Activates notifications on the event or status changes described by the expressions. Notifications are sent in XML format to the specified URL. Up to 15 expressions may be registered for each of 3 feedback IDs.

ID: <1..3>

The ID of this particular feedback request.

URL(r): <S: 1, 256>

The URL to which notifications are to be sent.

Expression.1..15: <S: 1, 256>

The events or status change to be notified. Valid Expressions are:

Status/Ethernet	Status/Calls	Event/CallDisconnected
Event/	Status/NTP	Status/Registrations
Event/CallFailure	Event/Bandwidth	Status/LDAP
Status/Zones	Event/RegistrationAdded	Event/Locate
Status/Feedback	Event/CallAttempt	Event/RegistrationRemoved
Event/ResourceUsage	Status/ExternalManager	Event/CallConnected
Event/RegistrationFailure	Event/AuthenticationFailure	

Example: **xCommand FeedbackRegister ID: 1 URL: "http://192.168.0.1/feedback/" Expression.1: "Status/Calls" Expression.2: "Event/CallAttempt"**

FindRegistration

Returns information about the registration associated with the specified alias. The alias must be registered on the VCS on which the command is issued.

Alias(r): <S: 1, 60>

The alias that you wish to find out about.

Example: **xCommand FindRegistration Alias: "john.smith@example.com"**

ForceConfigUpdate

Performs an xCommand DefaultValuesSet Level: 2 on the specified peer, and then forces the relevant configuration on the peer to be updated to match that of the cluster master.

PeerId: <1..6>

The index of the cluster peer to be updated.

Example: **xCommand ForceConfigUpdate PeerId: 1**

LinkAdd

Adds and configures a new link.

LinkName(r): <S: 1, 50>

Assigns a name to this link.

Node1: <S: 1, 50>

Specifies the first zone or subzone to which this link will be applied.

Node2: <S: 1, 50>

Specifies the second zone or subzone to which this link will be applied.

Pipe1: <S: 1, 50>

Specifies the first pipe to be associated with this link.

Pipe2: <S: 1, 50>

Specifies the second pipe to be associated with this link.

Example: **`xCommand LinkAdd LinkName: "Subzone1 to UK" Node1: "Subzone1" Node2: "UK Sales Office" Pipe1: "512Kb ASDL"`**

LinkDelete

Deletes a link.

LinkId(r): <1..3000>

The index of the link to be deleted.

Example: **`xCommand LinkDelete LinkId: 2`**

ListPresentities

Returns a list of all the presentities being watched by a particular subscriber.

Subscriber(r): <S:1, 255>

The URI of the subscriber who is watching.

Example: **`xCommand ListPresentities Subscriber: "john.smith@example.com"`**

ListSubscribers

Returns a list of all subscribers who are watching for the presence information of a particular presentity.

Presentity(r): <S:1, 255>

The URI of the presentity being watched.

Example: **`xCommand ListSubscribers Presentity: "mary.jones@example.com"`**

Locate

Runs the VCS's location algorithm to locate the endpoint identified by the given alias, searching locally, on neighbors, and on systems discovered through the DNS system, within the specified number of 'hops'. Results are reported back through the xFeedback mechanism, which must therefore be activated before issuing this command (e.g. xFeedback register event/locate).

Alias(r): <S: 1, 60>

The alias associated with the endpoint you wish to locate.

HopCount(r): <0..255>

The hop count to be used in the search.

Protocol(r): <H323/SIP>

The protocol used to initiate the search.

SourceZone: <S: 1, 50>

The zone from which to simulate the search request. Choose from the Default Zone (an unknown remote system), the Local Zone (a locally registered endpoint) or any other configured neighbor, traversal client or traversal server zone.

Authenticated: <Yes/No>

Whether the search request should be treated as authenticated or not.

SourceAlias: <S: 0, 60>

The source alias to be used for the search request. Default: xcom-locate

Example: **`xCommand Locate Alias: "john.smith@example.com" HopCount: 15 Protocol: SIP SourceZone: LocalZone Authenticated: Yes SourceAlias: alice@example.com`**

Log

Sets logging levels on specific modules.

Note: this command is intended for developer use only.

Module: <S:0, 255>

The name of the module.

TraceLevel: <Default/Error/Warn/Info/Debug/Trace>

The level of tracing to use on the specified module. Default returns the trace level to its default value.

Example: **`xCommand Log Module: "foo" TraceLevel: Error`**

LogPersist

Saves the current log levels so that they will persist over a restart.

This command has no parameters.

Example: **`xCommand LogPersist`**

OptionKeyAdd

Adds a new option key to the VCS. These are added to the VCS in order to add extra functionality, such as increasing the VCS's capacity. Contact your Cisco representative for further information.

Key(r): <S: 0, 90>

Specifies the option key of your software option.

Example: **`xCommand OptionKeyAdd Key: "1X4757T5-1-60BAD5CD"`**

OptionKeyDelete

Deletes a software option key from the VCS.

OptionKeyId(r): <1..64>

Specifies the ID of the software option to be deleted.

Example: **`xCommand OptionKeyDelete OptionKeyId: 2`**

PipeAdd

Adds and configures a new pipe.

PipeName(r): <S: 1, 50>

Assigns a name to this pipe.

TotalMode: <Unlimited/Limited/NoBandwidth>

Determines whether or not this pipe is enforcing total bandwidth restrictions. *NoBandwidth*: no bandwidth available; no calls can be made using this pipe. Default: Unlimited.

Total: <1..100000000>

If this pipe has limited bandwidth, sets the maximum bandwidth (in kbps) available at any one time on the pipe. Default: 500000.

PerCallMode: <Unlimited/Limited/NoBandwidth>

Determines whether or not this pipe is limiting the bandwidth of individual calls. *NoBandwidth*: no bandwidth available; no calls can be made using this pipe. Default: Unlimited.

PerCall: <1..100000000> If this pipe has limited per-call bandwidth, sets the maximum amount of bandwidth (in kbps) available for any one call. Default: 1920.

Example: **`xCommand PipeAdd PipeName: "512k ADSL" TotalMode: Limited Total: 512 PerCallMode: Limited PerCall: 128`**

PipeDelete

Deletes a pipe.

PipeId(r): <1..1000>

The index of the pipe to be deleted.

Example: **`xCommand PipeDelete PipeId: 2`**

PolicyServiceAdd

Adds a policy service.

Name(r): <S: 0, 50>

Assigns a name to this Policy Service.

Description: <S: 0, 64>

A free-form description of the Policy Service.

Protocol: <HTTP/HTTPS>

Specifies the protocol used to connect to the remote service. Default: HTTP

Verify: <On/Off>

Controls X.509 certificate checking and mutual authentication between this VCS and the policy service. When enabled, the server's FQDN or IP address, as specified in the address field, must be contained within the server's X.509 certificate (in either the Subject Common Name or the Subject Alternative Name attributes). Default: On

CRLCheck: <On/Off>

Controls certificate revocation list checking of the certificate supplied by the policy service. When enabled, the server's X.509 certificate will be checked against the revocation list of the certificate authority of the certificate. Default: Off

Address: <S: 0, 128>

Specifies the IP address or Fully Qualified Domain Name (FQDN) of the remote service.

Path: <S: 0, 255>

Specifies the URL of the remote service.

UserName: <S: 0, 30>

Specifies the user name used by the VCS to log in and query the remote service.

Password: <S: 0, 82>

Specifies the password used by the VCS to log in and query the remote service. The maximum plaintext length is 30 characters, which will then be encrypted.

DefaultCPL: <S: 0, 255>

The CPL used by the VCS when the remote service is unavailable. Default: <reject status='403' reason='Service Unavailable'/>

Example: **`xCommand PolicyServiceAdd Name: "Conference" Description: "Conference service" Protocol: HTTP Verify: On CRLCheck: On Address: "service.server.example.com" Path: "service" UserName: "user123" Password: "password123" DefaultCPL: "<reject status='403' reason='Service Unavailable'/>"`**

PolicyServiceDelete

Deletes a policy service.

PolicyServiceId(r): <1..5>

The index of the policy service to be deleted.

Example: **`xCommand PolicyServiceDelete PolicyServiceId: 1`**

RemoveRegistration

Removes a registration from the VCS.

Registration: <1..3750>

The index of the registration to be removed.

RegistrationSerialNumber: <S: 1, 255>

The serial number of the registration to be removed.

Example: **`xCommand RemoveRegistration RegistrationSerialNumber: "a761c4bc-25c9-11b2-a37f-0010f30f521c"`**

Restart

Restarts the VCS without a full system reboot.

This command has no parameters.

Example: **`xCommand Restart`**

RouteAdd

Adds and configures a new IP route (also known as a static route).

Address(r): <S: 1, 39>

Specifies an IP address used in conjunction with the prefix length to determine the network to which this route applies. Default: 32

PrefixLength(r): <1..128>

Specifies the number of bits of the IP address which must match when determining the network to which this route applies.

Gateway(r): <S: 1, 39>

Specifies the IP address of the gateway for this route.

Interface: <Auto/LAN1/LAN2>

Specifies the LAN interface to use for this route. *Auto*: the VCS will select the most appropriate interface to use. Default: Auto

Example: **`xCommand RouteAdd Address: "10.13.8.0" PrefixLength: 32 Gateway: "192.44.0.1"`**

RouteDelete

Deletes a route.

RouteId(r): <1..50>

The index of the route to be deleted.

Example: **`xCommand RouteDelete RouteId: 1`**

SearchRuleAdd

Adds a new search rule to route searches and calls toward a zone or policy service.

Name(r): <S: 0, 50>

Descriptive name for the search rule.

ZoneName: <S: 0, 50>

The zone or policy service to query if the alias matches the search rule.

Description: <S: 0, 64>

A free-form description of the search rule.

Example: **xCommand SearchRuleAdd Name: "DNS lookup" ZoneName: "Sales Office" Description: "Send query to the DNS zone"**

SearchRuleDelete

Deletes a search rule.

SearchRuleId(r): <1..2000>

The index of the search rule to be deleted.

Example: **xCommand SearchRuleDelete SearchRuleId: 1**

SecureModeOff

Turns secure mode off - removes all audit information that contains sensitive information, such as log files and call, status and login history records.

This command has no parameters.

Example: **xCommand SecureModeOff**

SecureModeOn

Turns secure mode on - certain features and login accounts will be unavailable.

This command has no parameters.

Example: **xCommand SecureModeOn**

SIPRouteAdd

Adds a route that will cause SIP messages matching the given criteria to be forwarded to the specified IP address and port.

Note: this command is intended for developer use only.

Method(r): <S:0, 64>

SIP method to match to select this route (e.g. INVITE, SUBSCRIBE).

RequestLinePattern(r): <S:0, 128>

Regular expression to match against the SIP request line.

HeaderName(r): <S:0, 64>

Name of SIP header field to match (e.g. Event).

HeaderPattern(r): <S:0, 128>

Regular expression to match against the specified SIP header field.

Authenticated(r): <On/Off>

Whether to forward authenticated requests. *On*: only forward requests along route if incoming message has been authenticated. *Off*: always forward messages that match this route. Default: Off

Address(r): <S:0, 39>

Specifies the IP address of the next hop for this route, where matching SIP requests will be forwarded.

Port(r): <1..65534>

Specifies the port on the next hop for this route to which matching SIP requests will be routed. Default: 5060

Transport(r): <UDP/TCP/TLS>

Determines which transport type will be used for SIP messages forwarded along this route.

Tag(r): <S:0, 64>

Tag value specified by external applications to identify routes that they create.

Example: **`xCommand SIPRouteAdd Method: "SUBSCRIBE" RequestLinePattern: ".*@(%localdomains%|%ip%)" HeaderName: "Event" HeaderPattern: "(my-event-package)(.*)" Authenticated: On Address: "127.0.0.1" Port: 22400 Transport: TCP Tag: "Tag1"`**

SIPRouteDelete

Deletes an existing SIP route, identified either by the specified index or tag.

Note: this command is intended for developer use only.

SipRouteId: <1..20>

The index of the SIP route to be deleted.

Tag: <S:0, 64>

Tag value specified by external applications to uniquely identify routes that they create.

Example: **`xCommand SIPRouteDelete SipRouteId: Tag: "Tag1"`**

SubZoneAdd

Adds and configures a new subzone.

SubZoneName(r): <S: 1, 50>

Assigns a name to this subzone.

TotalMode: <Unlimited/Limited/NoBandwidth>

Determines whether this subzone has a limit on the total bandwidth of calls being used by its endpoints at any one time. *NoBandwidth*: no bandwidth available. No calls can be made to, from, or within this subzone. Default: Unlimited.

Total: <1..100000000>

Sets the total bandwidth limit (in kbps) of this subzone (applies only if the mode is set to *Limited*). Default: 500000.

PerCallInterMode: <Unlimited/Limited/NoBandwidth>

Sets bandwidth limits for any one call to or from an endpoint in this subzone. *NoBandwidth*: no bandwidth available. No calls can be made to or from this subzone. Default: Unlimited.

PerCallInter: <1..100000000>

Specifies the bandwidth limit (in kbps) on any one call to or from an endpoint in this subzone (applies only if the mode is set to *Limited*). Default: 1920.

PerCallIntraMode: <Unlimited/Limited/NoBandwidth>

Sets bandwidth limits for any one call between two endpoints within this subzone. *NoBandwidth*: no bandwidth available. No calls can be made within this subzone. Default: Unlimited.

PerCallIntra: <1..100000000>

Specifies the bandwidth limit (in kbps) for any one call between two endpoints within this subzone (applies only if the mode is set to Limited). Default: 1920.

Example: **`xCommand SubZoneAdd SubZoneName: "BranchOffice" TotalMode: Limited Total: 1024 PerCallInterMode: Limited PerCallInter: 512 PerCallIntraMode: Limited PerCallIntra: 512`**

SubZoneDelete

Deletes a subzone.

SubZoneId(r): <1..1000>

The index of the subzone to be deleted.

Example: **`xCommand SubZoneDelete SubZoneId: 2`**

SubZoneMembershipRuleAdd

Adds and configures a new membership rule.

Name(r): <S: 1, 50>

Assigns a name to this membership rule.

Type(r): <Subnet/AliasPatternMatch>

The type of address that applies to this rule. *Subnet*: assigns the device if its IP address falls within the configured IP address subnet. *Alias Pattern Match*: assigns the device if its alias matches the configured pattern.

SubZoneName(r): <S: 1, 50>

The subzone to which an endpoint is assigned if its address satisfies this rule.

Description: <S: 0, 64>

A free-form description of the membership rule.

Example: **`xCommand SubZoneMembershipRuleAdd Name: "Home Workers" Type: Subnet SubZoneName: "Home Workers" Description: "Staff working at home"`**

SubZoneMembershipRuleDelete

Deletes a membership rule.

SubZoneMembershipRuleId(r): <1..3000>

The index of the membership rule to be deleted.

Example: **`xCommand SubZoneMembershipRuleDelete SubZoneMembershipRuleId: 1`**

TransformAdd

Adds and configures a new transform.

Pattern(r): <S: 1, 60>

Specifies the pattern against which the alias is compared.

Type: <Exact/Prefix/Suffix/Regex>

How the pattern string must match the alias for the transform to be applied. *Exact*: the entire string must exactly match the alias character for character. *Prefix*: the string must appear at the beginning of the alias. *Suffix*: the string must appear at the end of the alias. *Regex*: the string is treated as a regular expression. Default: Prefix

Behavior: <Strip/Replace/AddPrefix/AddSuffix>

How the alias is modified. *Strip*: removes the matching prefix or suffix from the alias. *Replace*: substitutes the matching part of the alias with the text in the replace string. *AddPrefix*: prepends the replace string to the alias. *AddSuffix*: appends the replace string to the alias. Default: Strip

Replace: <S: 0, 60>

The text string to use in conjunction with the selected Pattern behavior.

Priority: <1..65534>

Assigns a priority to the specified transform. Transforms are compared with incoming aliases in order of priority, and the priority must be unique for each transform. Default: 1

Description: <S: 0, 64>

A free-form description of the transform.

State: <Enabled/Disabled>

Indicates if the transform is enabled or disabled. Disabled transforms are ignored. Default: Enabled

Example: **`xCommand TransformAdd Pattern: "example.net" Type: suffix Behavior: replace Replace: "example.com" Priority: 3 Description: "Change example.net to example.com" State: Enabled`**

TransformDelete

Deletes a transform.

TransformId(r): <1..100>

The index of the transform to be deleted.

Example: **`xCommand TransformDelete TransformId: 2`**

UserLoginGroupAdd

Creates a new user login group.

Name(r): <S: 0, 128>

Defines the name of a user group that determines which access rights members of the group have after they have been successfully authenticated to use the VCS.

Access(r): <None/ReadWrite>

Defines the access level for members of the specified user group. *None*: no access allowed. *ReadWrite*: configuration can be viewed and changed. Default: ReadWrite

Example: **`xCommand UserLoginGroupAdd Name: "FindMeAccounts" Access: ReadWrite`**

UserLoginGroupDelete

Deletes a user login group.

UserLoginGroupId(r): <1..15>

The index of the user login group to be deleted.

Example: **xCommand UserLoginGroupDelete UserLoginGroupId: 1**

WarningAcknowledge

Acknowledges an existing warning.

Note: this command is intended for developer use only.

WarningID(r): <S:36, 36>

The warning ID

Example: **xCommand WarningAcknowledge WarningID: "ab3d63f6-c0bb-4a9c-a121-e683abfedff0"**

WarningLower

Lowers a warning.

Note: this command is intended for developer use only.

WarningID(r): <S:36, 36>

The warning ID.

Example: **xCommand WarningLower WarningID: "ab3d63f6-c0bb-4a9c-a121-e683abfedff0"**

WarningRaise

Raises a warning.

Note: this command is intended for developer use only.

WarningID(r): <S:36, 36>

The warning ID.

WarningText(r): <S:0, 255>

The description of the warning.

Example: **xCommand WarningRaise WarningID: "ab3d63f6-c0bb-4a9c-a121-e683abfedff0" WarningText: "Module foo is malfunctioning"**

ZoneAdd

Adds and configures a new zone.

ZoneName(r): <S: 1, 50>

Assigns a name to this zone.

Type(r): <Neighbor/TraversalClient/TraversalServer/ENUM/DNS>

Determines the nature of the specified zone, in relation to the local VCS. Neighbor: the new zone will be a neighbor of the local VCS. *TraversalClient*: there is a firewall between the zones, and the local VCS is a traversal client of the new zone. *TraversalServer*: there is a firewall between the zones and the local VCS is a traversal server for the new zone. *ENUM*: the new zone contains endpoints discoverable by ENUM lookup. *DNS*: the new zone contains endpoints discoverable by DNS lookup.

Example: **xCommand ZoneAdd ZoneName: "UK Sales Office" Type: Neighbor**

ZoneDelete

Deletes a zone.

ZoneId(r): <1..1000>

The index of the zone to be deleted.

Example: **`xCommand ZoneDelete ZoneId: 2`**

ZoneList

A diagnostic tool that returns the list of zones (grouped by priority) that would be queried, and any transforms that would be applied, in a search for a given alias.

Note that this command does not change any existing system configuration.

Alias(r): <S: 1, 60>

The alias to be searched for.

Example: **`xCommand ZoneList Alias: "john.smith@example.com"`**

xStatus command reference

The **xStatus** group of commands are used to return information about the current status of the system. Each **xStatus** element returns information about one or more sub-elements.

The following section lists all the currently available **xStatus** commands, and the information that is returned by each command.

To obtain information about the existing status, type:

- **xStatus** to return the current status of all status elements
- **xStatus <element>** to return the current status for that particular element and all its sub-elements
- **xStatus <element> <sub-element>** to return the current status of that group of sub-elements

To obtain information about the **xStatus** commands, type:

- **xStatus ?** to return a list of all elements available under the **xStatus** command

xStatus elements

The current xStatus elements are:

- Alternates
- Applications
- Calls
- Ethernet
- ExternalManager
- Feedback
- FindMeManager
- H323
- IP
- LDAP
- Links
- Loggers
- NTP
- Options
- Pipes
- Policy
- Registrations
- ResourceUsage
- SIP
- SystemUnit
- TURN
- Warnings
- Zones

Each element has the sub-elements as described below:

Alternates

```
Alternates:
    Peer [1..6]: {Hidden for Peer [n] when Peer [n] is self}
        Status: <Active/Failed/Unknown>
        Cause: {visible if status is Failed} <No response from gatekeeper/DNS
resolution failed/Invalid IP address>
```

```
        Address: <IPv4Addr/IPv6Addr>
        Port: <1..65534>
        LastStatusChange: <Seconds since boot/Date Time>
```

Applications

```
Applications:
   Presence:
      UserAgent:
         Status: <Inactive/Initializing/Active/Failed>
         Presentity:
            Count: <0..2500>
      Server:
         Publications:
            Presentities:
               Count: <0..10000>
               Max: <0..10000>
               Presentity [1..10000]:
                  URI: <S: 1,255>
                  Document:
                     Count: <1..10>
         Subscriptions:
            Subscribers:
               Count: <0..n>
               Max: <0..n>
               Subscriber [1..2500]:
                  URI: <S: 1,255>
                  Subscription:
                     Count: <1..100>
            Count: <1..2500>
            Max: <1..2500>
            Expired: <1..2500>
         Presentities:
            Count: <0..10000>
            Max: <0..10000>
            Presentity [1..10000]:
               URI: <S: 1,255>
               Subscriber:
                  Count: <1..100>
   ConferenceFactory:
      Status: <Inactive/Initializing/Active/Failed>
      NextId: <0.. 4294967295>
   External
      Status:
         Relay:
            Registrations:
               Count: <1..2500>
            Subscriptions:
               Count: <1..2500>
            User 1:
               Alias: <S: 1,255>
               Subscription:
                  State: <Subscription request sent/Subscription
successful/Subscription error response/Failed/Notification received/Active>
```

```
            Registration:
               State: <Registered/Not Registered>
            Presence:
               OCS:
                  Machine:
                     State: <Offline/Available/Undefined>
                  User:
                     State: <Undefined/Busy>
                  VCS:
                     State: <Offline/Online/In a call/Undefined>
      LastUpdate:
         Time: <date time>
         SecondsSinceLastRefresh: <seconds>
```

Calls

```
Calls:
   Call <1..900>:
      SerialNumber: <S: 1,255>
      Tag: <S: 1,255>
      State: <Connecting/Connected/Disconnecting>
      StartTime: <Seconds since boot/Date Time>
      Duration: <Time in seconds, precision in seconds>
      Legs:
         Leg [1..300]:
            Protocol: <H323/SIP>
            H323: {visible if Protocol = H323}
               CallSignalAddress: <IPv4Addr/[IPv6Addr]>:<1..65534>
               Aliases:
                  Alias [1..50]:
                     Type: <E164/H323Id>
                     Value: <S: 1,60>
            SIP: {visible if Protocol = SIP}
               Address: <IPv4Addr/[IPv6Addr]>:<1..65534>
               Transport: <UDP/TCP/TLS/undefined>
               Aliases:
                  Alias [1..50]:
                     Type: <URL>
                     Value: <S: 1,60>
            EncryptionType: <None/DES/AES-128>
            CheckCode: <S: 1,60> {visible if Leg = H323 and call is interworked}
            Targets:
               Target [1..1]:
                  Type: <E164/H323Id/URL>
                  Value: <S: 1,60>
            BandwidthNode: <S: 1,50 Node name>
            Registration:
               ID: <1..2500>
               SerialNumber: <S: 1,255>
               VendorInfo: <S: 1,255>
   Sessions:
      Session: [1..300:]
         Status: <Unknown/Searching/Failed/Cancelled/Completed/Active/Connected>
         MediaRouted: <True/False>
```

```
         CallRouted: <True/False>
         Participants:
            Leg: <1..300> {2 entries}
         Bandwidth:
            Requested: <0..100000000> kbps
            Allocated: <0..100000000> kbps
         Route:
            Zone/Link: <S: 1,50 Node name> {0..150 entries}
         Media {visible if MediaRouted = True}
            Channels
               Channel [1..n]
                  Type: <AUDIO/VIDEO/DATA/BFCP/H224/UNKNOWN>
                  Protocol: <S: 1,20> {RTP Payload Type}
                  Rate: <0.. 4294967295> bps
                  Packets:
                     Forwarded:
                        Total: <0.. 4294967295>
                  Incoming:
                     Leg: <1..300>
                  Outgoing:
                     Leg: <1..300>
```

Ethernet

```
Ethernet [1..2]:
   MacAddress: <S: 17>
   Speed: <10half/10full/100half/100full/1000full/down>
   IPv4:
      Address: <IPv4Addr>
      SubnetMask: <IPv4Addr>
   IPv6:
      Address: <IPv6Addr>
```

External Manager

```
External Manager:
   Status: <Inactive/Initializing/Active/Failed>
   Cause: {visible if status is Failed} <Failed to connect to external manager / No
response from external manager / Failed to register to external manager / DNS
resolution failed >
   Address: <IPv4Addr/IPv6Addr >
   Protocol: HTTP
   URL: <S: 0, 255>
```

Feedback

```
Feedback [1..3]:
   Status: <On/Off>
   URL: <S: 1,255>
   Expression: <S: 1,127> {0..15 entries}
```

FindMeManager

```
FindMeManager:
   Mode: <Off/Local/Remote>
   Status: <Active/Inactive/Unknown> {visible if Remote}
   Address: <1..1024> {Visible if Remote}
```

H323

```
H323:
   Registration:
      Status: <Active/Inactive/Failed>
      IPv4: {Visible if Status=Active}
         Address: <IPv4Addr> {1..2 entries}
      IPv6: {Visible if Status=Active}
         Address: <IPv6Addr> {1..2 entries}
      OutOfResources: <True/False>
   CallSignaling:
      Status: <Active/Inactive/Failed>
      IPv4: {Visible if Status=Active}
         Address: <IPv4Addr> {1..2 entries}
      IPv6: {Visible if Status=Active}
         Address: <IPv6Addr> {1..2 entries}
   Assent:
      CallSignaling:
         Status: <Active/Inactive/Failed>
         IPv4: {Visible if Status=Active}
            Address: <IPv4Addr> {1..2 entries}
         IPv6: {Visible if Status=Active}
            Address: <IPv6Addr> {1..2 entries}
   H46018:
      CallSignaling:
         Status: <Active/Inactive/Failed>
         IPv4: {Visible if Status=Active}
            Address: <IPv4Addr> {1..2 entries}
         IPv6: {Visible if Status=Active}
            Address: <IPv6Addr> {1..2 entries}
```

IP

```
IP:
   Protocol: <IPv4/IPv6/Both>
   IPv4:
      Gateway: <IPv4Addr>
   IPv6:
      Gateway: <IPv6Addr>
   DNS:
      Server [1-5]:
         Address: <IPv4Addr/IPv6Addr>
      Domain: <S: 0, 128>
```

LDAP

```
LDAP:
   Status: <Inactive/Initializing/Active/Failed>
   Cause: {visible if status is Failed} <Failed to connect to LDAP server / The LDAP
server does not support TLS. / Failed to establish a TLS connection to the LDAP
server. Please check that the LDAP server certificate is signed by a CA, and that CA
is included on the CA certificate installed on the VCS. / Failed to authenticate with
LDAP server / A valid CA certificate for the LDAP database has not been uploaded;
this is required for connections via TLS / No server address configured>
   Address: <IPv4Addr/IPv6Addr>
   Port: <1..65534>
```

Links

```
Links:
   Link [1..100]:
      Name: <S: 1,50 Link name>
      Bandwidth:
         LocalUsage: <0..100000000>
         ClusterUsage: <0..100000000>
      Calls:
         Call [0..900]: {0..900 entries}
            CallSerialNumber: <S: 1,255>
```

Loggers

```
Loggers
   Logger [1..6]
      Module:
      TraceLevel:
```

NTP

```
NTP:
   Status: <Inactive/Initializing/Active/Failed>
   Cause: {visible if status is Failed} <No response from NTP server/ DNS resolution
failed>
   Address: <IPv4Addr/IPv6Addr>
   Port: <1..65534>
   Last Update: <date-time>
   Last Correction: <Time in seconds, precision in seconds>
```

Options

```
Options:
   Option [1-64]:
      Key: <S: 1, 90>
      Description: <S: 1, 128>
```

Pipes

```
Pipes:
   Pipe [1..1000]:
      Name: <S: 1,50 Pipe name>
      Bandwidth:
         LocalUsage: <0..100000000>
         ClusterUsage: <0..100000000>
      Calls:
         Call [0..900]: {0..900 entries}
            CallID: <S: 1,255>
```

Policy

```
PolicyServices:
   PolicyService [1..5]:
      Name: <S: 1,50 Policy name>
      Status: <Active/Inactive>
      URL: <S: 1,255>
      LastUsed: <Time not set/Date Time>
      Peers:
         Peer [1..3]:
            Host: <S: 0,255>
            Status: <Active/Failed>
            Reason: <S: 0,255>
            LastStatusChange: <Time not set/Date Time>
```

Registrations

```
Registrations:
   Registration [1..3750]:
      Protocol: <H323/SIP>
      Node: <S: 1,50 Node name>
      SerialNumber: <S: 1,255>
      CreationTime: <Date Time>
      Duration: <Time in seconds, precision in seconds>
      SecondsSinceLastRefresh: <1..65534> {visible if Protocol is SIP}
      SecondsToExpiry <1..65534> {visible if Protocol is SIP}
      VendorInfo: <S: 1,255>
      H323: {Visible if Protocol is H323}
         Type: <Endpoint/MCU/Gateway/Gatekeeper/MCUGateway>:
         CallSignalAddresses:
            Address: <IPv4Addr/[IPv6Addr]>:<1..65534>
         RASAddresses:
            Address: <IPv4Addr/[IPv6Addr]>:<1..65534>
            Apparent: <IPv4Addr/[IPv6Addr]>:<1..65534>
         Prefix: <S: 1,20> {0..50 entries}
         Aliases:
            Alias [1..50]:
               Type: <E164/H323Id/URL/Email/GW Prefix/MCU
Prefix/Prefix/Suffix/IPAddress>
               Origin: <Endpoint/LDAP/Combined>
               Value: <S: 1,60>
         Traversal: <Assent/H46018> {visible for Traversal registration}
      SIP: {Visible if Protocol is SIP}
```

```
         AOR: <S: 1,128>
         Contact: <S: 1,255>
         Path:
            URI [1..10]: <S: 1,255>
```

ResourceUsage

```
ResourceUsage:
   Calls:
      Traversal:
         Current: <0..150>
         Max: <0..150>
         Total: <0..4294967295>
      NonTraversal:
         Current: <0..750>
         Max: <0..750>
         Total: <0..4294967295>
   Registrations:
      Current: <0..3750>
      Max: <0..3750>
      Total: <0..4294967295>
   TURN:
      Relays:
         Current: <0..1400>
         Max: <0..1400>
         Total: <0..4294967295>
```

SIP

```
SIP:
   Ethernet [1..2]
      IPv4:
         UDP:
            Status: <Active/Inactive/Failed>
            Address: <IPv4Addr>
         TCP:
            Status: <Active/Inactive/Failed>
            Address: <IPv4Addr>
         TLS:
            Status: <Active/Inactive/Failed>
            Address: <IPv4Addr>
      IPv6:
         UDP:
            Status: <Active/Inactive/Failed>
            Address: <IPv6Addr>
         TCP:
            Status: <Active/Inactive/Failed>
            Address: <IPv6Addr>
         TLS:
            Status: <Active/Inactive/Failed>
            Address: <IPv6Addr>
```

SystemUnit

```
SystemUnit:
   Product: TANDBERG VCS
   Uptime: <Time in seconds>
   SystemTime: <Time not set/date-time>
   TimeZone: <GMT or one of 300 other timezones>
   LocalTime: <local-date-time>
   Software:
      Version: X<n>
      Build: <Number/Uncontrolled>
      Name: "Release"
      ReleaseDate: <Date>
      ReleaseKey <ReleaseKey>
      Configuration:
         NonTraversalCalls: <0..500>
         TraversalCalls: <0..100>
         Registrations: <0..2500>
         Expressway: <True/False>
         Encryption: <True/False>
         Interworking: <True/False>
         FindMe: <True/False>
         DeviceProvisioning: <True/False>
         DualNetworkInterfaces: <True/False>
         AdvancedAccountSecurity: <True/False>
         StarterPack: <True/False>
      Hardware:
         Version: 1.0
         SerialNumber: <hardware serial number>
```

TURN

```
TURN:
   Server:
      Status: <Active/Inactive>
      Interface [1..2]:
         Address: <IPv4Addr/IPv6Addr>
      Relays:
         Count: <0..1400>
         Relay [1..1400]:
            Address: <IPv4Addr/IPv6Addr>
            Client:
               Address: <IPv4Addr/IPv6Addr>
            CreationTime: <Date Time>
            ExpireTime: <Date Time>
            Permissions:
               Count: <0..65535>
               Permission [0..65535]:
                  Address: <IPv4Addr/IPv6Addr>
                  CreationTime: <Date Time>
                  ExpireTime: <Date Time>
            Channels:
               Count: <0..65535>
               Channel [0..65535]:
                  ID: <1..65535>
```

```
            Peer:
               Address: <IPv4Addr/IPv6Addr>
            CreationTime: <Date Time>
            ExpireTime: <Date Time>
      Counters:
         Received:
            Requests:
               Total: <0..65535>
               Allocate: <0..65535>
               Refresh: <0..65535>
               Permission: <0..65535>
               ChannelBind: <0..65535>
         Sent:
            Responses:
               Total: <0..65535>
               Allocate: <0..65535>
               Refresh: <0..65535>
               Permission: <0..65535>
               ChannelBind: <0..65535>
            Errors:
               Total: <0..65535>
               Allocate: <0..65535>
               Refresh: <0..65535>
               Permission: <0..65535>
               ChannelBind: <0..65535>
         Media:
            Forwarded:
               From: <0..65535>
               To: <0..65535>
            Errors:
               From:
                  NoChannel: <0..65535>
                  NoPermission: <0..65535>
                  InvalidType: <0..65535>
                  FilterFailure: <0..65535>
               To:
                  NoChannel: <0..65535>
                  NoPermission: <0..65535>
                  InvalidType: <0..65535>
                  FilterFailure: <0..65535>
```

Warnings

```
Warnings:
   Warning [1..n]:
      ID: <S: 36,36>
      Reason: <S: 0,255>
      State: <Acknowledged/Unacknowledged>
```

Zones

```
Zones:
   DefaultZone:
```

```
      Name: "DefaultZone"
      Bandwidth:
         LocalUsage: <0..100000000>
         ClusterUsage: <0..100000000>
      Calls: {visible only if there are calls}
         Call [0..900]: {0..900 entries}
            CallId: <S: 1,255>
   LocalZone:
      DefaultSubZone:
         Name: "DefaultSubZone"
         Bandwidth:
            LocalUsage: <0..100000000>
            ClusterUsage: <0..100000000>
         Registrations: {0..3750 entries } {visible only if there are registrations}
            Registration: <1..3750>
               SerialNumber: <S: 1,255>
         Calls: {visible only if there are calls}
            Call [0..900]: {0..900 entries}
               CallId: <S: 1,255>
      TraversalSubZone:
         Name: "TraversalSubZone"
         Bandwidth:
            LocalUsage: <0..100000000>
            ClusterUsage: <0..100000000>
         Calls: {visible only if there are calls}
            Call [0..900]: {0..900 entries}
               CallId: <S: 1,255>
      ClusterSubZone:
         Name: "ClusterSubZone"
         Bandwidth:
            LocalUsage: <0..100000000>
            ClusterUsage: <0..100000000>
         Calls: {visible only if there are calls}
            Call [0..900]: {0..900 entries}
               CallId: <S: 1,255>
      SubZone: [0..100]
         Name: <S: 1,50 Node name>
         Bandwidth:
            LocalUsage: <0..100000000>
            ClusterUsage: <0..100000000>
         Registrations: {0..3750 entries} {visible only if there are registrations}
            Registration: <1..3750>
               SerialNumber: <S: 1,255>
         Calls: {visible only if there are calls}
            Call [0..900]: {0..900 entries}
               CallId: <S: 1,255>
   Searches:
      Current:
      Total:
      Dropped:
   Zone [1..1000]:
      Name: <S: 1,50 Node name>
      Bandwidth:
         LocalUsage: <0..100000000>
         ClusterUsage: <0..100000000>
      Status: <Active/Failed/Warning>
```

```
      Cause: {Visible if status is Failed or Warning} <System unreachable/ Systems
unreachable>
      Type: <Neighbor/TraversalClient/TraversalServer/ENUM/DNS>
      Neighbor: {Visible if Type is Neighbor}
         Peer [1..6]:
            H323: {visible if H323 Mode=On for Zone}
               Status: <Unknown/Active/Failed>
               Cause: {visible if Status is Failed} <No response from gatekeeper/DNS
resolution failed/Invalid IP address>
               Address: <IPv4Addr/IPv6Addr> {One Address line per address from DNS
lookup}
               Port: <1..65534>
               LastStatusChange: <Time not set/Date Time>
            SIP: {visible if SIP Mode=On for Zone}
               Status: <Unknown/Active/Failed>
               Cause: {visible if Status is Failed} <No response from gatekeeper/DNS
resolution failed/Invalid IP address>
               Address: <IPv4Addr/IPv6Addr> {One Address line per address from DNS
lookup}
               Port: <1..65534>
               LastStatusChange: <Time not set/Date Time>
      TraversalClient: {Visible if Type is TraversalClient}
         Peer [1..6]:
            H323: {visible if H323 Mode=On for Zone}
               Status: <Unknown/Active/Failed>
               Cause: {visible if Status is Failed} <No response from gatekeeper/DNS
resolution failed/Invalid alias/Authentication Failed/Invalid IP address>
               Address: <IPv4Addr/IPv6Addr> {One Address line per address from DNS
lookup}
               Port: <1..65534>
               LastStatusChange: <Time not set/Date Time>
            SIP: {Visible if SIP Mode=On for Zone}
               Status: <Unknown/Active/Failed>
               Cause: {visible if Status is Failed} <No response from neighbor/ DNS
resolution failed>
               Address: <IPv4Addr/IPv6Addr> {One Address line per address from DNS
lookup}
               Port: <1..65534>
               LastStatusChange: <Time not set/Date Time>
      TraversalServer: {visible if Type is TraversalServer}
         SIP:
            Port: <Active/Inactive>
         H323:
            Port: <Active/Inactive>
         Peer [1..6]:
            H323: {visible if H323 Mode=On for Zone}
               Status: Active
               Address: <IPv4Addr/IPv6Addr> {One Address line per address from DNS
lookup}
               Port: <1..65534>
               LastStatusChange: <Time not set/Date Time>
            SIP: {visible if SIP Mode=On for Zone}
               Status: Active
               Address: <IPv4Addr/IPv6Addr> {One Address line per address from DNS
lookup}
               Port: <1..65534>
```

```
         LastStatusChange: <Time not set/Date Time>
Calls: {0..900 entries}
   Call [0..900]:
   CallID: <S: 1,255>
```

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.

xConfiguration command reference 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.

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
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>

Configuration item	Reset value
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>
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>

Configuration item	Reset value
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

Policy services

Policy services are typically used in 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.

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

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

Policy service request parameters

The Cisco VCS sends HTTP(S) GET requests to the specified policy service. The parameters and their values within each request depend upon the type of request. For example a Registration Policy request will contain a different set of parameters than a Call Policy request.

The following table lists the possible parameters contained within a request and indicates with an **X** in which request types that parameter is included.

Parameter name	Values	Registration Policy	Search rules	Call Policy
ALIAS		X		
ALLOW_ INTERWORKING	TRUE / FALSE		X	X
AUTHENTICATED	TRUE / FALSE		X	X
AUTHENTICATED_ SOURCE_ALIAS			X	X
AUTHENTICATION_ USER_NAME			X	X
CLUSTER_NAME		X	X	X
DESTINATION_ALIAS			X	X
GLOBAL_CALL-SERIAL_NUMBER			X	X
LOCAL_CALL_ SERIAL_NUMBER			X	X
METHOD	INVITE / ARQ / LRQ / OPTIONS / SETUP / REGISTER		X	X
NETWORK_TYPE	IPV4 / IPV6		X	X
POLICY_TYPE		REGISTRATION	SEARCH	ADMIN
PROTOCOL	SIP / H323	X	X	X
REGISTERED_ALIAS			X	X
SOURCE_ADDRESS		X	X	X

Parameter name	Values	Registration Policy	Search rules	Call Policy
TRAVERSAL_TYPE	TYPE_[UNDEF / ASSENTSERVER / ASSENTCLIENT / H460SERVER / H460CLIENT / TURNSERVER / TURNCLIENT / ICE]		X	X
UNAUTHENTICATED_SOURCE_ALIAS			X	X
UTCTime		X	X	X
ZONE_NAME			X	X

Policy service responses

The Cisco VCS expects the response from the policy service to include an item of CPL which will then be validated and processed by the Cisco VCS.