Cisco TelePresence Video Communication Server X7.0.3

Software release notes

D14851.06

January 2012

Contents

Document revision history

Revision	Date	Description
01	August 2011	Initial release for X7.0.
02	October 2011	X7.0.1 maintenance release.
03	October 2011	Included resolution details for CSCts80342 / CSCts82540 (resolved in X7.0).
04	October 2011	Update for open caveat CSCtt41169; SSH and SCP clients removed.
05	November 2011	X7.0.2 maintenance release.
06	January 2012	X7.0.3 maintenance release.

Introduction

These release notes describe the features and capabilities included in the Cisco TelePresence Video Communication Server (Cisco VCS) software version X7.0.3.

Upgrading to VCS X7.0.n

CAUTION: If you are upgrading a cluster, you must follow the directions in the X7.0.n "Cluster Creation and Maintenance" Cisco VCS deployment guide (document D14367), otherwise the cluster will not synchronize.

There is a **software dependency** between **VCS X7.n** and **TMS 12.6 or later**. If you are running Cisco TelePresence Management Suite (Cisco TMS) with Provisioning or FindMe, or your Cisco VCSs are clustered and you want to upgrade your Cisco VCS to X7.0 or later, you must also upgrade Cisco TMS to TMS 12.6 or later, see the table below.

Deployment using Provisioning, Clustering or FindMe				
Software version	**TMS 12.1**	**TMS 12.2**	**TMS 12.5**	**TMS 12.6 or later**
X4.n	√	√	X	X
X5.0, X5.1.1	X	X	√	X
X5.2	X	X	X	√
X6.n	X	X	X	√
X7.n	X	X	X	√

Note: If you are running TMS 12.5 you must upgrade it to 12.6 or later before upgrading to VCS X7.n.

Note: You should backup your system before upgrading. If you later need to downgrade to an earlier release you will have to restore a backup made against that previous release (see "Upgrading from X6.1 to X7" for more information about backing up X6.1 systems).

It is **vital** that you upgrade the **Cisco VCS** and **Cisco TMS** correctly – instructions for the upgrade are documented in the "Updating to" section of this document.

Upgrading a non-clustered Cisco VCS to X7.0.n from X5.0 or earlier

If you are currently running VCS X5.0 or earlier you must first upgrade to X5.2 and then upgrade from X5.2 to X7.0.n.

You can only upgrade directly to X7.0.n if you have version X5.1 or later.

Device authentication

Upgrades from release X5.2 or earlier to X7.0.n

If device authentication is not enabled when the Cisco VCS is upgraded to X7.0.n, the upgrade process will configure all zones and subzones (except the default zone) on the Cisco VCS with authentication set to 'Treat as authenticated'. This ensures that:

- CPL continues to work as expected
- Caller ID can be set to the FindMe ID for calls originating from endpoints specified in a FindMe
- The provisioning request is challenged by the provisioning server

If you are upgrading from X6.n to X7.0.n your existing authentication configuration will not be changed.

Note that if TMS Agent (rather than the Cisco VCS) challenges for authentication of provisioning data, the initial presence publication by Movi (if running Movi version 4.1 or earlier) will fail; to publish Movi presence, users must manually set their presence status after logging in.

Cisco VCS Starter Pack Express

If you have a Cisco VCS Starter Pack Express and you want to provision devices then you must set the Default Zone to “Check credentials” (or “Treat as authenticated”). This is because the starter pack provisioning server that runs on the Cisco VCS checks, but does not challenge for, credentials.

Cisco VCS upgrades where authentication is already enabled

If device authentication is enabled when the Cisco VCS is upgraded to X7.0.n, the upgrade process will configure the Cisco VCS with authentication set to ‘Check credentials’. This means that:

- CPL continues to work as expected
- Caller ID can be set to the FindMe ID for calls originating from endpoints specified in a FindMe
- The provisioning request is challenged by the Cisco VCS

Recommendations

Device authentication

You should review your whole network and consider whether authentication should be enabled for all endpoints and enable authentication where possible.

CPL modifications

In CPL, the ‘origin’ field is a short-hand for ‘authenticated-origin’. You are recommended to update your CPL to make it explicit whether the CPL is looking at the authenticated or unauthenticated origin. If CPL is required to look at the unauthenticated origin (e.g. when checking non-authenticated callers) the CPL must use “unauthenticated-origin”. To check the authenticated origin (only available for authenticated or “treat as authenticated” devices) the CPL should use “authenticated-origin”. Note that:

- authenticated-origin is available for endpoints where ‘Check credentials’ succeeded, and for endpoints where they are registered to a ‘Treat as authenticated’ subzone
- unauthenticated-origin is available for all endpoints, whether authenticated or unauthenticated

Upgrading from X6.1 to X7.n

Important note for Cisco VCS units delivered with X6.1 pre-installed

As with upgrading from any Cisco VCS release, you should first backup your system before upgrading. However, if your system was delivered with X6.1 pre-installed, you must make some configuration changes before using the backup process.

You do not need to use the procedure below if you do not have X6.1 installed or your installation of X6.1 is the result of an upgrade from a previous release.

To ensure that all of your data is backed up:

1. Log in to the Cisco VCS as root user.
2. Enter the following commands:
   a. mkdir /tandberg/persistent/oti
   b. mkdir /tandberg/persistent/management
3. Exit the root account.

You can now log into the web user interface and backup your system as normal via **Maintenance > Backup and restore**, and then upgrade the Cisco VCS using the X7.0.n “Cluster Creation and Maintenance” Cisco VCS deployment guide, or by following the “Updating to X7.0.n” instructions in this document.

New features in X7

X7.0.3

This is a maintenance release.

X7.0.2

This is a maintenance release.

X7.0.1

This is a maintenance release.

X7.0

Device authentication using an Active Directory Service for Movi endpoints configurable via web interface

The ability to authenticate devices via a direct connection between the Cisco VCS and an Active Directory Service (ADS) can now be configured via the web interface.

Shared cluster licenses

Call licenses are now shared across the entire Cisco VCS cluster.

Traversal and non-traversal call license option keys are still installed on each individual peer and are subject to per-peer limits, but the licenses are available to all peers in the cluster. Note that any other option keys (FindMe, for example) must still be installed identically on each cluster peer, as before.

Note that if a Cisco VCS peer loses its connection to the cluster, the shareable licenses installed on that peer will remain available to the rest of the cluster peers for two weeks from the time the cluster lost contact with the peer.

Microsoft Edge Server support via B2BUA for Microsoft OCS/Lync

Support for Microsoft Edge Server communications has been added via the introduction of a back-to-back user agent (B2BUA) application. The B2BUA provides interworking between Microsoft ICE (used when MOC / Lync clients communicate through the Edge Server) and media for communications with standard video endpoints. The B2BUA also provides call hold, call transfer and Multiway support for calls with OCS/Lync clients, and can share FindMe presence information with OCS/Lync.

The B2BUA replaces the deprecated “Microsoft Office Communication Server” zone profile. After upgrade, any OCS zones, if enabled, will still work as in previous software versions. However, users are recommended to migrate to the new B2BUA functionality by following the *Microsoft OCS 2007, Lync 2010 and Cisco VCS* deployment guide (document reference D14269).

Presence User Agent

You can now configure the **Default published status for registered endpoints** to be either *Online* or *Offline*. This is the presentity status published by the Presence User Agent for registered endpoints when they are not "In-Call".

Enhanced SIP registration expiry controls

New SIP registration settings on the **SIP** page (**VCS configuration > Protocols > SIP > Configuration**) allow you to configure how the Cisco VCS calculates the expiry period for SIP registration requests. These settings enable the system to balance the load of registration and re-registration requests. They can be configured separately for standard and Outbound registration connections.

These settings supersede the previous **Registration expire delta** setting.

Improved diagnostics

A range of tools have been introduced to improve troubleshooting.

Diagnostic logging

Additional diagnostic tools have been introduced under a new **Maintenance > Diagnostics** menu structure:

- There is a **Diagnostic logging** tool (**Maintenance > Diagnostics > Diagnostic logging**) that can be used to assist in troubleshooting system issues. It allows you to generate a diagnostic log of system activity over a period of time, and then to download the log so that it can be sent to your Cisco customer support representative.
- You can configure log levels for specific **Network Log** and **Support Log** modules. Note that these are advanced logging configuration options and should only be changed on the advice of Cisco customer support.
- The existing **System snapshot** and **Incident reporting** options have been moved under the new **Maintenance > Diagnostics** menu structure.
- The **System snapshot** tool can now generate three types of snapshot: system status, system logs or a full snapshot.

Network utilities

The following network utility tools have been introduced under **Maintenance > Tools > Network utilities**:

- **Ping**: allows you to check that a particular host system is contactable from the Cisco VCS and that your network is correctly configured to reach it.
- **Traceroute**: allows you to discover the route taken by a network packet sent from the Cisco VCS to a particular destination host system.
- **DNS lookup**: allows you to check which domain name server (DNS server) is responding to a request for a particular hostname.

Alarms (warnings)

- Warnings are now referred to as alarms.
- The alarm icon in the menu bar indicates the current number of unacknowledged alarms.
- The **Alarms** page indicates when an alarm was last raised and the number of times it has occurred since the last restart.
- In a clustered Cisco VCS system the **Alarms** page shows all of the alarms raised by any of the cluster peers. Only those alarms that have been raised by the "current" peer can be acknowledged.

GRUU (Globally Routable User Agent URI) support

The Cisco VCS has implemented the Public GRUU element of RFC 5627: *Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP)*.

A GRUU is a SIP URI that can be used anywhere on the internet to route a request to a specific AOR instance. Note that the registering domain must be globally routable in order for the Cisco VCS to support GRUU.

Improved DNS subsystem

- The DNS subsystem within the Cisco VCS has been re-structured and improved to be standards compliant.
- It provides the ability to specify explicit upstream DNS servers for specified domains.

Improved NTP synchronization

The Cisco VCS can now be configured to connect to up to 5 standards-based NTP server addresses.

TMS Agent database credentials included within local authentication database lookups

If the Cisco VCS is enabled for device provisioning (it has the Device Provisioning option key installed and therefore has a TMS Agent database), then in addition to any manually created entries, the Cisco VCS now checks credentials stored within that VCS's TMS Agent database when the device authentication database type is set to *Local database*.

This makes it easier to enable authentication on the Cisco VCS when provisioning is using passwords originating from TMS.

Other enhancements and usability improvements

- You can now configure up to 200 SIP domains.
- You can now configure up to 10,000 local authentication database credentials.
- Full support of RFC 5806: any SIP diversion headers received in a 302 response are now maintained in the outgoing INVITE message.
- Improved zone status reporting: the zones summary page now shows separate SIP and H.323 connection status information.
- Table sorting indicators: tabular displays now indicate by which column each table is sorted.
- A filter facility has been added to the **Subzones** list page.
- Chrome web browser is now supported; Internet Explorer 6 is no longer officially supported.
- The administrator no longer has to log out and log back in again after reconfiguring DNS server addresses.
- There is a new **Call signaling routed mode** advanced zone profile setting for neighbor zones. It controls whether the zone always takes the signaling or uses the system-wide **Call routed mode** setting.
- There is a new **H.323 call signaling port** advanced zone profile setting for neighbor zones. It identifies the call signaling port on the neighbor system to use if **Automatically respond to H.323 searches** is set to *On*.
- SSH and SCP clients are no longer available in the VCS operating system.

Resolved caveats

The following issues were found in previous releases and were resolved in X7.n.

Resolved in X7.0.3

Internal reference	Identifier	Summary
59485	CSCtu06577	**VCS may crash and report a SIGSEGV fault**: **Symptoms**: Cisco VCS may crash, and an alarm be raised stating that an unexpected software error was detected in app with a SIGSEGV fault. A crash report will also be generated and when this is analyzed a call to sha1_block_data_order() in libcrypto is seen in the trace back. **Conditions**: This was on a Cisco VCS release X7.0.1 **Workaround**: There is no workaround at this time.
121590	CSCtt94053	**No presence PUBLISH generated by PUA in SIP->H323 interworked call in VCS cluster**: **Symptoms**: sometimes in-call presence is not published by PUA for H.323 calls. **Conditions**: H.323 endpoint must register to a cluster peer and the call must come in through another peer in the cluster. (If the call arrives on the same peer to which the endpoint is registered, the in-call presence will be fine.) **Workaround**: dual register endpoints as SIP and H.323.
121639	CSCtw61291	**The VCS fails to listen on call signaling ports**: **Symptoms**: The VCS fails to listen on call signaling ports after a reboot / restart / upgrade. **Conditions**: The issue is due to a race condition as ports are assigned during bootup. It occurs rarely. **Workaround**: It could potentially be cleared by a restart.
122016	CSCtx24762	**The CPU load of the VCS increases dramatically in X7 when %localdomains% is used in pattern matching.** **Symptoms**: The VCS has a high CPU load, reducing responsiveness. **Conditions**: The issue is due to the increase in the number of local domains permitted in X7, and the way in which the %localdomains% keyword is expanded in pattern matching. **Workaround**: Explicitly list domains rather than use %localdomains%.

Resolved in X7.0.2

Internal reference	Identifier	Summary
119002	CSCts38224	**Security Issue in Apache (CVE-2011-3192 and CVE-2011-3348)** A denial of service vulnerability has been found in the way the multiple overlapping ranges are handled by the Apache HTTPD server. Multiple Cisco products could be affected by this vulnerability. Mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Intelligence companion document for this Advisory: http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=24024 This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110830-apache.shtml. **PSIRT Evaluation**: the Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation

Internal reference	Identifier	Summary
		are 7.8/7.8: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:C/E:H/RL:U/RC:C CVE ID CVE-2011-3192 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html The Cisco VCS now uses Apache 2.2.21, which addresses these security advisories.
116841	CSCtr84963	**Possible loss of grace period for call licenses (in cluster configuration):** If a cluster peer loses contact with its cluster, the remaining peers can continue to use the non-contactable peer's licenses for a 2-week grace period. But, if another peer within the cluster is restarted during that period, that restarted peer will not be able to make use of the non-contactable peer's licenses for the remainder of the grace period. This issue is resolved; grace periods are now observed if a peer is restarted.
118282	CSCts05797	**VCS SIP/H323 interworking does not adhere to change in SIP payload type after hold/resume**: interworked calls can lose video after a hold/resume if there is a change in the SIP payload type. VCS now manages correctly a change in the payload type.
118308	CSCts15739	**Cisco VCS challenges B2BUA SUBSCRIBE for authentication when Default Zone is set to "Check credentials":** When a Cisco VCS is set up with the Default Zone set to "Check credentials" and the X7.0 B2BUA feature is also set up on the same VCS, any SUBSCRIBE messages sent from the B2BUA will result in a 407 Proxy Authentication Required response from the VCS. Eventually the B2BUA gives up sending SUBSCRIBE messages and this results in failed subscription states for B2BUA/Lync users. This does not affect customers still using OCS Relay (rather than the B2BUA). This issue is resolved; subscribe messages now include a P-Asserted-Identity header.
118340	CSCtt14099	**Duo Video fails from an H.323 endpoint**: Duo Video from an H.323 endpoint can fail when using BFCP and interworking with SIP. This issue is now resolved.
121174	CSCtt41169	**VCS rejects outgoing call from specific device registered on it** Requests to FindMe from an H.323 device which has a large number of aliases associated with it will fail. This is especially relevant to large MCUs and MPSs. This issue is now resolved.
119052	CSCts60535	**Encryption status under call summary is shown as none**: active calls always show the encryption status as none. When the call is completed the call history shows the correct status. The correct encryption status is now displayed for active calls.

Resolved in X7.0.1

Internal reference	Identifier	Summary
120030	CSCts87885	**DNS lookup problems that make VCS appear to have a hardware fault**: for a Cisco VCS Expressway running X7.0 with DNS zones configured (e.g. for business to business calling), it has been observed when there are DNS lookup issues that the VCS may get into a hung state. When the DNS lookup problem occurs the VCS does not respond to Web, SSH, Telnet or Serial access. This issue has now been resolved.

Resolved in X7.0

Security-related issues

Internal reference	Identifier	Summary
53663	CSCtr80182	**DNS cache poisoning attacks CVE-2008-1447**: previous releases of Cisco VCS were vulnerable to CVE-2008-1447. Version X7.0 has been upgraded to use dnsmasq 2.57 which has resolved the issue.
85524	CSCtr80196	**OpenSSL Ciphersuite Downgrade Attack CVE-2010-4180 and Openssl clienthello vulnerability CVE-2011-0014**: previous releases of Cisco VCS were vulnerable to CVE-2010-4180 and CVE-2011-0014. Version X7.0 has been upgraded to use openssl 1.0.0d, which has resolved the issue.
86485	CSCtr32396	**VCS Command Injection Vulnerability** **Symptoms**: administrator entered values within the administrative interfaces of the Cisco VCS may not be properly sanitized. This could allow a malicious administrator to cause arbitrary commands to be executed on the underlying system. **Conditions**: a device is running an affected version of Cisco VCS. **Workaround**: restrict access to the administrative interfaces to trusted users only. **Further Problem Description**: while this issue may allow an authenticated, remote attacker to cause arbitrary commands to be executed. Any successful command execution is performed under the restricted 'nobody' account, restricting the direct impact of this issue. Malicious values that are entered via the command line interface may not be immediately executed, and instead the malicious actions may be performed the next time an administrator accesses a page containing the malicious value via the administrative web interface. **PSIRT Evaluation**: the Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.5/5.4: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:P/I:P/A:P/E:F/RL:OF/RC:C CVE ID CVE-2011-2538 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html
86676	CSCtr80205	**PHP vulnerabilities CVE-2010-4697 and CVE-2006-7243**: previous releases of Cisco VCS were vulnerable to CVE-2010-4697 and CVE-2006-7243. Version X7.0 has been upgraded to use php 5.3.5 which has resolved the issue.
86985 / 119916	CSCts82540 CSCts80342	A vulnerability exists in Cisco TelePresence Video Communication Server (VCS) due to improper validation of user-controlled input to the web-based administrative interface. User-controlled input supplied to the login page via the HTTP User-Agent header is not properly sanitized for illegal or malicious content prior to being returned to the user in dynamically generated web content. A remote attacker could exploit this vulnerability to perform reflected cross-site scripting (XSS) attacks. Billy Hoffman from Zoompf, Inc. discovered this vulnerability and Ben Feinstein from Dell SecureWorks reported it to Cisco. Cisco greatly appreciates the opportunity to work with researchers on security vulnerabilities and welcome the opportunity to review and assist in product reports. Cisco TelePresence Video Communication Server Software versions earlier than X7.0 are affected. This vulnerability has been corrected in Cisco TelePresence Video Communication Server Software version X7.0. The Cisco Security Response has been published at:

Internal reference	Identifier	Summary
		http://www.cisco.com/warp/public/707/cisco-sr-20111012-vcs.shtml **PSIRT Evaluation**: the Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/4.1: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:P/A:N/E:F/RL:U/RC:C CVE ID CVE-2011-3294 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

Other

Internal reference	Identifier	Summary
85593	CSCtr80162	**External policy**: when editing a policy service under the **VCS configuration > Dial plan > Policy services** web page it is not possible to change the password used for remote authentication. The password can however be changed via the CLI interface or by deleting and then recreating the whole policy service with the new password. This issue has now been resolved.
85692	CSCtr80200	**Truncated SNMP object value**: the SNMP sysObjectID scalar MIB object value was being returned truncated by the Cisco VCS. Instead of returning 1.3.6.1.4.1.5596.130.6.4.1 it actually returned 1. This meant that if Cisco TMS was configured to find devices using SNMP (the default configuration) it would not discover the Cisco VCS. This issue has now been resolved.
88084	CSCtr80209	**Incorrect responses to attempts to communicate with the Cisco VCS on ports in range 4369–4380**: the issue where the Cisco VCS incorrectly responded with an ISAKMP message if a device attempted to connect to a VCS port in the range 4369–4380 has been resolved.
88493	CSCtr80179	**Internal server error when unregistering and blocking an alias**: resolved the issue where use of the **Unregister and block** button on the **Registration details** page when using a Registration Policy of Deny List caused an internal server error.
88177	CSCtl98133	**Cisco VCS not responding to OLC**: resolved the issue where the Cisco VCS was not responding to OLC (Open Logical Channel) messages from H.323 endpoints when interworking SIP/H.323 calls.

Open caveats

The following issues currently apply to this version of the Cisco VCS.

Internal reference	Identifier	Summary
69881	CSCtr80148	**TURN server port configuration**: if the port of the TURN server is changed while the TURN server is running, then the TURN server must be restarted before the port change takes effect. This can be achieved by turning TURN services Off and then On again from the TURN configuration page.
79180	CSCtr28842	**Out of date call and registration status:** call and registration status displays can be out of date if the status changes mid-call or mid-registration. Some of the call/registration status information that is displayed is only updated when the call ends.
83660	CSCtt13556	**When a new policy service is created or modified its status defaults to Active**: **Symptom**: when a policy service is created or modified its status defaults to Active. It can remain as Active for 30 seconds - long enough to convince the user that it really is active, even if it subsequently fails. **Workaround**: after creating or modifying a policy service, wait 30 seconds and then refresh the policy services page.
84054	CSCts02660	**Seconds since last refresh and Seconds to expiry do not update on the web interface**: the **Seconds since last refresh** and **Seconds to expiry** fields on the **Registration details** web page do not get updated if a manual refresh of the web page is performed.
86253	CSCtr80175	**Cisco VCS Starter Pack Express and remote authentication of login account credentials requires lower case usernames:** when setting up user (FindMe) accounts you must enter the account usernames in lower case. If usernames are created with mixed or upper case the user will not be able to log in to the Cisco VCS. Note that passwords are case sensitive. This issue applies only if you have a Cisco VCS Starter Pack Express and are using remote (LDAP) authentication of login account credentials.
87105	CSCtr37987	**During normal operation the system temp alarm got raised on the VCS but didn't clear**: The user might see the following in the /var/log/messages: hwstatus: Event="Application Crash" Detail="Traceback (most recent call last):, File '/bin/hwstatus.py'
88103	CSCtr77670	**SIP DNS zone defaults to UDP**: searches made through DNS zones use UDP for A record lookups. They do this even if UDP is disabled at the SIP protocol level (on the SIP page). However, if SIP UDP is disabled, the call will not connect. This scenario is more likely to occur in new installations of X7 software which has SIP UDP disabled by default. The workaround is to enable SIP UDP.
88239	CSCtr80189	**Viewing web pages with IE8 in compatibility mode:** there are display problems with the Cisco VCS web interface when viewing web pages with IE8 in compatibility mode. The workaround is to switch off IE8 compatibility mode.
88376	CSCtr77658	**Cisco VCS sends SIP INFO for content channel without stream ID**: when interworking calls from H.323 to SIP, Fast Update Requests do not contain a stream ID.
115427	CSCtq73481	**SSH configuration allows for port forwarding**: **Symptoms**: SSH configuration allows port forwarding to be enabled. **Conditions**: none. **Workaround**: ensure that SSH access to VCS is only available to trusted users. **PSIRT Evaluation**: the Cisco PSIRT has assigned this bug the following CVSS

Internal reference	Identifier	Summary
		version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 1.4/1.3: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:L/Au:M/C:N/I:P/A:N/E:F/RL:U/RC:C No CVE ID has been assigned to this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html
115654	CSCtq81698	**VCS allows port overlap for disabled protocols in multi traversal zones**: **Symptom**: some messages will not traverse the traversal zone. **Conditions**: two (or more) traversal zones are configured with identical port numbers for a disabled protocol (such as SIP). **Workaround**: configure unique port numbers for each traversal zone and protocol (H323, SIP), even if the protocol is disabled.
116099	CSCtr84970	**"transferfindmeaccounts" script fails**: the "transferfindmeaccounts" script fails to complete successfully. This script is required if you need to change the **Cluster name** of your Cisco VCS and you are using FindMe (with or without Cisco TMS). There is no workaround for this problem; do not change the **Cluster name** if you are using FindMe.
116655	CSCtr27042	**dialedDigits returned in RRJ does not indicate the actual alias which is a duplicate:** **Conditions**: a Cisco TelePresence VCS configured as a H323 gatekeeper returns an RRJ when a H323 endpoint attempts to register with an alias already registered to the gatekeeper. Returning the RRJ due to duplicateAlias is correct but the dialedDigits value returned is the first terminalAlias, not the actual duplicate alias. **Workaround**: verify on the VCS which aliases are registered to the gatekeeper to determine where the duplicate alias resides.
116952	CSCtr84978	**Cisco VCS Starter Pack Express and B2BUA – FindMe users are not registered to Microsoft/OCS/Lync in a timely manner:** it can take up to 2 hours for FindMe users to be registered to Microsoft OCS/Lync. Note that this issue only occurs if the B2BUA is enabled on a Cisco VCS Starter Pack Express.
117230	CSCtr84966	**System snapshot requests can time out on web interface:** the system snapshot process can take several minutes to complete. During this time the web interface can time out. Therefore even though the snapshot file will have been successfully generated, the web interface will not provide the user with the option to save the snapshot file. **Workaround**: the snapshot file can be downloaded from the VCS unit via another tool such as scp.
118390	CSCts31410	**Phantom B2BUA calls appearing up in call status**: the Call status page (Status > Calls > Calls) can show phantom calls through the B2BUA. These are typically calls that were never established. Such calls remain visible on the Call status page until the Cisco VCS is next restarted.
118520, 118523	CSCts25438, CSCts25426	**B2BUA does not disconnect a call on 408 (Request Timeout) responses / does not support session timers (RFC 4028)** **Symptoms**: if a call is not properly cleared up with a BYE (either from the Cisco endpoint or the MOC/Lync client) then it is not cleared from the Cisco VCS. It remains visible under call status and if the Cisco VCS Expressway is used for TURN services the TURN session will remain.
120531	CSCtt17243	**Admin accounts not replicated across a cluster**: **Symptoms**: if a new administrator account is created on a cluster master peer, that same account is not created on the non-master peers. **Conditions**: problem exists from X5.2 and is fixed in X7.1. **Workaround**: after creating a new account on master peer, restart each non-

Internal reference	Identifier	Summary
		master peer in turn to activate the account. Make sure the non-master peer has completed its restart before restarting another peer.
120593	CSCtt17237	**"sip:" prefix is not stripped before CPL search**: Symptoms: sip: and/or h323: prefixes to URIs are "unexpectedly" part of the pattern match in CPL regexs. If deny rules are put in which do not explicitly cope with sip: or h323: prefixes hackers may be able to make calls that would have been expected to have been denied. **Conditions**: CPL regex rules in place to deny certain URIs, but do not explicitly include a test that allows a sip: or h.323: prefix. **Workaround**: for example, if the deny rule is to deny calls starting with a 9, instead of using a regex of: 9(.*) use: (.*:)?9(.*)
121214	CSCtt44554	**Format string vulnerability in tshell**: **Symptoms**: a format string vulnerability exists when parsing command line arguments passed to the tshell binary. This results in a segmentation fault. **Conditions**: the only way to pass arguments to tshell is when the user is logged in as root. **PSIRT Evaluation**: the Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 1.5/1.2: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:M/Au:S/C:N/I:N/A:P/E:F/RL:OF/RC:C No CVE ID has been assigned to this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html
121554	CSCtu02124	**NTP occasionally fails after VCS restart** **Symptom:** alarm indicating NTP unreachable but in actual fact the NTP process has failed to run up directly after a restart. **Diagnosis:** the stopping of the previous NTP process failed complete in time during the restart and so the socket is still in use when trying to start up the new NTP process. **Workaround:** a restart of the affected system solves this problem.
121673	CSCtu20349	**Starter Pack: after first SUBSCRIBE and NOTIFY from provisioning server, subsequent NOTIFYs do not get sent to Movi** **Symptom**: after registration, and first SUBSCRIBE and NOTIFY from provisioning server, subsequent NOTIFYs (following re-SUBSCRIBEs from Movi 4.3.5 or later) do not get sent to the Movi. Therefore Movi will not pick up any provisioning changes contained in the NOTIFY. **Scope**: in X7.0.n this is limited to Starter Pack deployments ONLY (TMS Agent / Argon deployments work fine without any problems). **Versions affected**: VCS X7.0.n Starter Pack with Movi 4.3.5 or later. This may affect E20 deployments, further testing is required. **Status**: fixed in X7.1. **Mitigations**: this problem does not affect call scenarios or the ability to make/receive calls. After 5 minutes, Movi should re-SUBSCRIBE after the initial SUBSCRIBE. Because it already has an existing registration, it will receive a new NOTIFY and pick up relevant updates. In E20 deployments the timeout will be 60 minutes instead of 5 minutes.
121976	CSCtu13020	**Need to disable automatic DST timezone change for Russia from autumn 2011**: **Symptoms**: DST changes are wrong in some parts of Russia from autumn 2011. **Conditions**: DST set to Russian area in an area where they have changed

Internal reference	Identifier	Summary
		timezone rules. **Workaround**: use a different timezone (for example Arabian GMT+4). **Additional Information**: effective from autumn 2011, Russia has reduced the number of timezones it uses. As part of this Russia is also changing the way it handles DST in some areas as a way of converging areas together; the changed areas will stay with summer timezone the whole year. The changed areas will no longer adhere to the automatic DST change rules installed in the VCS.

Interoperability

The systems below have been tested with this software release.

Gatekeepers / traversal servers

Equipment	Software revision
Cisco VCS	X6.1, X7.0
TANDBERG Gatekeeper	N6.3

Gateways

Equipment	Software revision
Cisco TelePresence ISDN Gateway	2.1(1.43)
Cisco TelePresence IP Gateway 3500 Series	2.0(1.11)
Cisco 2811 Router (ISDN+SIP)	15.0(1)M3

IP PBXs

Equipment	Software revision
Cisco Unified Communications Manager	8.6.1

MCUs

Equipment	Software revision
Cisco TelePresence MCU 4200	4.2
Cisco TelePresence MCU 4500	4.2
Cisco TelePresence MCU MSE 8420	4.2
Cisco TelePresence MCU MSE 8510	4.2
Cisco TelePresence Server	2.2

Streaming servers

Equipment	Software revision	Comments
Cisco TelePresence Content Server	S5.0	See Known limitations section

PC video

Equipment	Software revision
Cisco TelePresence Movi	4, 4.1, 4.2
Microsoft Office Communicator	2007 R2, Lync 2010

Endpoints

Equipment	Software revision	Comments
Cisco IP Video Phone E20	TE4.0.0 TE4.1.0	
Cisco TelePresence System EX90	TC4.1.0 TC4.2.0	
Cisco TelePresence System EX60	TC4.1.0 TC4.2.0	
Cisco TelePresence System Integrator C Series	TC4.1.0 TC4.2.0	
Cisco TelePresence System Profile MXP Series	F9.1	
LifeSize Room	4.6.0	See Known limitations section
Polycom VSX 7000	9.0.6.1	See Known limitations section
Polycom HDX 9000	3.0.0.2	See Known limitations section

Known limitations

Manufacturer	Equipment / Version / Protocol	Summary
Cisco	TelePresence Content Server versions earlier than S5.2	The SIP **Standard registration refresh minimum** setting introduced in VCS X7.0 has a default value of 45 seconds. Devices that request a value lower than the **Standard registration refresh minimum** setting will result in the registration being rejected with a 423 Interval Too Brief response. Any SIP devices, such as the Cisco TelePresence Content Server, that do not retry their registration request after receiving a 423 response will fail to register. The workaround is to set the **Standard registration refresh minimum** setting on the Cisco VCS to 30 seconds.
Polycom	HDX 9000 / 3.0.0.2 and 3.0.2 / SIP	An H.323 call routed via Cisco VCS will not connect when the destination is Polycom HDX registering using SIP. Polycom HDX does not send response to Cisco VCS interworked SIP INVITE request.
Polycom	VSX 7000 / 9.0.6.1 / SIP	A SIP call routed via the Cisco VCS to a Cisco TelePresence System Integrator C Series (using H.323) will connect, however the call will be disconnected when the VSX attempts to refresh the session. VSX attempts to refresh session using an UPDATE request, which is not supported by Cisco VCS.
Polycom	VSX 7000 / 9.0.6.1 / H.323	An H.323 call routed via the Cisco VCS will connect when the destination is Cisco IP Video Phone E20 (using SIP), however no video will be seen on the E20. Polycom VSX does not open the media channel that is signaled during call set up.
Polycom	VSX / 8.5.x ; v500 / 8.5.x	Multiplexed media is not supported.
Lifesize	Room / 4.6.0 / SIP	An H.323 call routed via Cisco VCS will be disconnected when the H.323 party puts the call on-hold. Lifesize Room (SIP) incorrectly responds to Cisco SDP (media capability) offer. This issue is resolved in Lifesize Room version 4.8.3.
Lifesize	Room / 4.6.0 / SIP	A Movi SIP call routed via Cisco VCS will connect, however no video will be seen on the Lifesize Room. Lifesize Room (SIP) incorrectly responds to Cisco SDP (media capability) offer. This issue is resolved in Lifesize Room version 4.8.3.
Lifesize	Room / 4.6.0 / H.323	A C20 or E20 SIP call routed via Cisco VCS will connect, however no video will be seen on the Lifesize Room. C20 and E20 do not send media to Lifesize after call is connected. This issue is resolved in Lifesize Room version 4.8.3.
Lifesize	Room / 4.6.0 and 4.8.3 / H.323	A Movi SIP call routed via Cisco VCS will connect, however no video will be seen on the LifeSize Room system if an HD camera is used and the requested bandwidth is > 1MBps.
TANDBERG	Gatekeeper	**TANDBERG Gatekeeper interoperability**: If a TANDBERG Gatekeeper is configured as a client in a traversal relationship with a Cisco VCS running X3.0 or later, then it is recommended that the Gatekeeper be

Manufacturer	Equipment / Version / Protocol	Summary
		upgraded to N6.1. If the Gatekeeper is not upgraded, it may occasionally restart when a call is attempted.
TANDBERG	Border Controller	**TANDBERG Border Controller interoperability**: if a TANDBERG Border Controller is configured as a server in a traversal relationship with a Cisco VCS running X3.0 or later, then it is recommended that the Border Controller be upgraded to Q6.1. If the Border Controller is not upgraded, it may occasionally restart when a call is attempted.
Mozilla	Firefox Version 4.0 and later	It is not possible to access the Cisco VCS HTTPS web interface in Mozilla Firefox Version 4.0 using a raw IPv6 address. It is possible with IPv4 addresses and in earlier versions of Firefox, or if a hostname is used instead of the raw IPv6 address. This is being tracked by Mozilla as bug 633001.

Updating to X7.0.n

CAUTION: If you are upgrading a cluster, you must follow the directions in the X7.0.n "Cluster Creation and Maintenance" Cisco VCS deployment guide (document D14367), otherwise the cluster will not synchronize.

Prerequisites and software dependencies

Cisco VCS and Cisco TMS software dependency

There is a software dependency between VCS X7.n and TMS 12.6 or later. If you are running Cisco TMS with Provisioning or FindMe, or your Cisco VCSs are clustered and you want to upgrade your Cisco VCS to X7.n or later, you must also upgrade Cisco TMS to TMS 12.6 or later.

The X7.0.n "Cluster creation and maintenance" deployment guide (document D14367) contains full instructions on how to upgrade to VCS X7.0.n and TMS 12.6 or later. Please use these instructions accompanied by the TMS upgrade procedures found in the relevant Cisco TMS Installation and Getting Started Guide.

If you are running TMS 12.5 you must upgrade it to 12.6 or later before upgrading to VCS X7.n.

You must use the procedures in the preceding documents if you use any of the following features:

- Clustering, or
- Device provisioning, or
- FindMe (with Cisco TMS managing Cisco VCS)

For other Cisco VCS deployments you may follow the Basic Cisco VCS X7.0.n upgrade procedure below.

Note that if you are running a single Cisco VCS with FindMe (without clustering or Cisco TMS) you can follow the Basic Cisco VCS X7.0.n upgrade procedure below. Note, if you configure FindMe on a single VCS with no replication to TMS and at a later date you include this Cisco VCS in a cluster you will have to re-enter your FindMe accounts as they will be overwritten by Cisco TMS. To avoid this problem you are recommended to use Cisco TMS 12.6 or later and Cisco VCS X7.0.n and replicate your Cisco VCS FindMe accounts with Cisco TMS.

Basic Cisco VCS X7.0.n upgrade procedure

Follow this procedure for upgrading Cisco VCS to X7.0.n, only if *all* of the following apply:

- The Cisco VCS is not part of a cluster, and
- Provisioning is not in use, and
- Cisco TMS is not managing the Cisco VCS
- Cisco VCS is currently X5.1.1 or later

Note: It is recommended that if FindMe™ is used that it is replicated with Cisco TMS. This allows a standalone Cisco VCS to be clustered in the future and the FindMe™ data kept. (If the FindMe™ data is not replicated with Cisco TMS, if the Cisco VCS is ever clustered the FindMe™ data from the Cisco VCS will be lost).

This procedure upgrades the Cisco VCS:

1. Backup the Cisco VCS.

   Note: You should backup your system before upgrading. If you later need to downgrade to an earlier release you will have to restore a backup made against that previous release.

Important note for Cisco VCS units delivered with X6.1 pre-installed

If your system was delivered with X6.1 pre-installed, you must make some configuration changes before using the backup process. You do not need to follow these additional steps if you do not have X6.1 installed or your installation of X6.1 is the result of an upgrade from a previous release. To ensure that all of your data is backed up:

a. Log in to the Cisco VCS as root user.

b. Enter the following commands:

   i. mkdir /tandberg/persistent/oti

   ii. mkdir /tandberg/persistent/management

c. Exit the root account.

2. Enable maintenance mode.
   Log in to the Cisco VCS as admin (SSH, telnet or serial), and at a command prompt, type:
   `xConfiguration SystemUnit Maintenance Mode: On`

3. Wait for all calls to clear and registrations to timeout.
   - If necessary, manually remove any calls that do not clear automatically (**Status > Calls**, click **Select all** and then click **Disconnect**).
   - If necessary, manually remove any registrations that do not clear automatically (**Status > Registrations > By device**, click **Select all** and then click **Unregister**).

4. Upgrade and restart the Cisco VCS (**Maintenance > Upgrade**).
   Note: The web browser interface may timeout during the restart process, after the progress bar has reached the end. (This may happen if the Cisco VCS initiates a disk file system check – which it does approximately once every 30 restarts.)

The upgrade is now complete and all Cisco VCS configuration should be as expected.

Upgrading from older releases

- It is not possible to upgrade from releases prior to X5.1 to X7.0.n. You must first upgrade to X5.2 and then to X7.0.n. See the X5.2 release note, document reference D50582, for details.

Getting help

If you experience any problems when configuring or using the Cisco VCS, consult the online help available within the UI of your Cisco VCS. The online help explains how the individual features and settings work.

If you cannot find the answer you need, check the web site at http://www.cisco.com/cisco/web/support/index.html where you will be able to:

- Make sure that the Cisco VCS is running the most up-to-date software.
- Find further relevant documentation, for example product user guides, printable versions of the online help, reference guides, and articles that cover many frequently asked questions.
- Get help from the Cisco Technical Support team. Click on **Technical Support Overview** for information on accessing Cisco Technical Services. Make sure you have the following information ready before raising a case:
  - The serial number and product model number of the unit (if applicable).
  - The software build number which can be found on the product user interface.
  - Your contact email address or telephone number.
  - A full description of the problem.

References and related documents

The following table lists documents and web sites referenced in this document. All product documentation can be found on www.cisco.com.

Name	Document reference
Cisco VCS Administrator Guide	D14049
Cisco VCS Command Reference	D14754
Cisco VCS Getting Started Guide	D14350
Cisco VCS Deployment Guide – Cluster creation and maintenance	D14367
Cisco VCS Deployment Guide – Basic Configuration – Single Cisco VCS Control	D14524
Cisco VCS Deployment Guide – Basic Configuration – Cisco VCS Expressway with Cisco VCS Control	D14651
Cisco VCS Deployment Guide – Cisco VCS Starter Pack Express	D14618
Cisco VCS Deployment Guide – FindMe	D14525
Cisco VCS Multiway Deployment Guide	D14366
Cisco TMS Provisioning Deployment Guide 13.0	D14368
Cisco VCS Deployment Guide – Cisco Unified Communications Manager with Cisco VCS using a SIP trunk	D14602
Cisco VCS Deployment Guide – Microsoft OCS 2007, Lync 2010 and Cisco VCS	D14269
Cisco VCS Deployment Guide – Microsoft OCS 2007, Cisco VCS Control and Cisco AM GW	D14652
Cisco VCS Deployment Guide – Authenticating Cisco VCS accounts using LDAP	D14526
Cisco VCS Deployment Guide – Certificate Creation and use with Cisco VCS	D14548
Cisco VCS Deployment Guide – ENUM dialing on Cisco VCS	D14465
Cisco VCS Deployment Guide – VCS and Cisco Unity Connection Voicemail Integration	D14809
Cisco VCS Deployment Guide – Authenticating Devices	D14819
Cisco TMS Release Note 13.0	D14741
Cisco TMS Installation Guide 13.0	D14389
Cisco TMS Administration Guide 13.0	D13741
Cisco TMS Provisioning Troubleshooting Guide	D14427

Appendix A — Supplemental notes

AES encryption support

The Cisco VCS uses one of the following software files for X4.0 or later software, where x<y_y_y> represents the software version (for example x7_0_0 represents X7.0).

Software	Software file properties
s42700x<y_y_y>	Supports AES
s42701x<y_y_y>	Does not support AES

Hardware shutdown procedure

The Cisco VCS uses a hard drive for storing logs and TMS Agent data. You are recommended to shut down the Cisco VCS prior to it being unplugged to ensure a clean shutdown process. This can be done from the web interface.

Network support

The Cisco VCS is an H.323 and SIP compliant device and is designed to be connected to an 802.3 IP network.

The first (or with dual network interface option, the first two) 802.3 Ethernet ports are used which are labeled LAN 1 (and LAN 2); the remaining two are currently unused. The Ethernet interfaces on the Cisco VCS support both manual configuration and auto speed and duplex detection for 1000Mbit Full Duplex, 100Mbit Full or Half Duplex or 10Mbit Full or Half Duplex.

It is recommended that speed and duplex setting should be set to auto unless the Ethernet switch that the Cisco VCS is connected to does not support auto-negotiation, if manually configured, ensure that full duplex is configured.

Restricting access to ISDN gateways (toll-fraud prevention)

Cisco VCS Expressway users should take appropriate action to restrict unauthorized access to ISDN gateway resources.

See the *Basic Configuration – Cisco VCS Expressway with Cisco VCS Control* deployment guide for information about how to do this.

SIP RFCs

The following RFCs are supported within the VCS X7 release:

RFC	Description
1889	RTP / RTCP
2327	SDP
2976	SIP INFO method
3261	Session Initiation Protocol

RFC	Description
3263	Locating SIP Servers
3264	An Offer/Answer Model with the Session Description Protocol (SDP)
3325	Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
3326	The Reason Header Field for the Session initiation Protocol (SIP)
3265	Session Initiation Protocol (SIP) – Specific Event Notification
3327	Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts
3515	Refer method
3581	An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing
3856	A Presence Event Package for the Session Initiation Protocol (SIP)
3863	Presence Information Data Format (PIDF)
3880	Call Processing Language (CPL): A Language for User Control of Internet Telephony Services
3891	Replaces header
3892	Referred-by header
3903	Session Initiation Protocol (SIP) Extension for Event State Publication
3944	H.350 Directory Services
4028	Session Timers in the Session Initiation Protocol
4479	A Data Model for Presence
4480	RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF)
5245	Interactive Connectivity Establishment (ICE)
5626	Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)
5627	Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP). Note that this RFC is only partially supported: Public GRUU is supported; Temporary GRUU is not supported.
5806	Diversion Indication in SIP

Getting the software

Customers should contact their Cisco maintenance provider for support and assistance with their Cisco products, including release keys and software files.

Web site www.cisco.com

Initial installation

Initial configuration of the Cisco VCS IP address, subnet and gateway can be accomplished through the installation wizard via the serial port or through the front LCD panel.

Layer 4 ports used

The following IP Layer 4 ports are used by the Cisco VCS:

Function	Type	Direction
SSH (Includes SCP)	22 TCP	Host → Cisco VCS
Telnet	23 TCP	Host → Cisco VCS
HTTP / XML	80 TCP	Host → Cisco VCS
HTTPS / XML	443 TCP	Host → Cisco VCS
SNMP (queries)	161 UDP	Host → Cisco VCS
DNS requests	1024:65535 UDP	Cisco VCS → Host
NTP	123 UDP	↔
Syslog	514 UDP	Cisco VCS → Host
LDAP communication	389 TCP	↔
LDAPS communication	636 TCP	↔
TMS cluster replication	443 TCP	Cisco TMS ↔ Cisco VCS
SSH cluster replication	22 TCP	Cisco VCS ↔ Cisco VCS
IPSEC cluster communication	500 UDP	Cisco VCS ↔ Cisco VCS
Intra-cluster communication	IP Protocol 51 (IPSec AH)	Cisco VCS ↔ Cisco VCS
Device provisioning	389 TCP	Cisco TMS → Cisco VCS
Device provisioning replication	8989 TCP	Cisco TMS → Cisco VCS
VCS database and TMS Agent	4444 TCP	Host → Cisco VCS
Gatekeeper discovery*	1718 UDP	Host → Cisco VCS
Gatekeeper RAS*	1719 UDP	↔
Incoming H.323 setup*	1720 TCP	Host → Cisco VCS
H.225/Q.931 call setup (non-traversal)*	15000:19999 TCP	↔
H.323 call signaling for Assent/H.460 traversal**	6001 UDP	Host → Cisco VCS
SIP call signaling for Assent traversal**	7001 TCP	Host → Cisco VCS
H.225/Q.931 call setup (Assent)*	2776 TCP	Host → Cisco VCS
H.225.Q931 call setup (H.460.18)*	1720 TCP	Host → Cisco VCS
H.245 call control (non-traversal)*	15000:19999 TCP	↔
H.245 call control (Assent)*	2776 TCP	Host → Cisco VCS
H.245 call control (H.460.18)*	2777 TCP	Host → Cisco VCS
H.323 / SIP media (RTP, RTCP) (non-traversal)*	50000:52399 UDP	↔
Media (Assent, H.460.19 multiplexed media)*	2776:2777 UDP	Host → Cisco VCS
Media (H.460.19 non-multiplexed media)*	50000:52399 UDP	Host → Cisco VCS
SIP call signaling*	5060 UDP	Host → Cisco VCS
SIP call signaling*	5060 TCP	Host → Cisco VCS
SIP call signaling*	5061 TLS	Host → Cisco VCS
SIP media (Assent)	2776:2777 UDP	Host → Cisco VCS

TURN services*	3478 UDP	Host → Cisco VCS
TURN media*	60000:61200 UDP	Host → Cisco VCS
B2BUA media*	56000:57000 UDP	↔
B2BUA communications with OCS/Lync*	65072 TLS	↔
B2BUA communications with VCS*	65070 TLS	Cisco VCS ↔ Cisco VCS
B2BUA communications with transcoders*	65080 TLS	↔
B2BUA OCS/Lync presence communications*	10011 TLS	↔
Ephemeral port range	40000:49999 TCP	Cisco VCS → Host
Outbound SIP connections*	25000:29999 TCP	Cisco VCS → Host

* All of these ports are default settings. Any ports denoted with * may be manually reconfigured, if desired. However, you are recommended not to adjust these ports unless specifically needed.

** These ports are the default settings for the first configured traversal zone. Each additional traversal zone increments the port values by 1. Any ports denoted with ** may be manually reconfigured, if desired. However, you are recommended not to adjust these ports unless specifically needed.