Cisco TelePresence Video Communication Server X7.2.2

Software release notes

D14851.14

April 2013

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.
07	March 2012	X7.1 release.
08	August 2012	X7.2 release.
09	August 2012	Added additional items that were resolved in X7.2, and open caveat CSCub66229.
10	September 2012	Added list of xConfiguration commands that are no longer supported in X7.2.
11	September 2012	Added known limitation interoperability issue for Polycom FX.
12	November 2012	X7.2.1 maintenance release.
13	March 2013	X7.2.2 maintenance release.
14	April 2013	Add CSCub76176 to list of resolved issues.

Introduction

These release notes describe the features and capabilities included in the Cisco TelePresence Video Communication Server (Cisco VCS) software version X7.2.2.

Upgrading to VCS X7.2.n

Read the "Open caveats" section before upgrading. You can only upgrade directly to X7.n if you have version X6.0 or later.

CAUTION: If you are upgrading a cluster, you must follow the directions in the X7.2 “Cluster Creation and Maintenance” 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.n 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 12.6-13.1**	**TMS 13.2**
X5.2	✓	✓
X6.n	✓	✓
X7.0.n	✓	✓
X7.1 / X7.2 (TMS Agent legacy mode)	✓	✓
X7.1 / X7.2 (TMS Provisioning Extension mode)	X	✓

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.

It is **vital** that you upgrade the **Cisco VCS** and **Cisco TMS** correctly – instructions for the upgrade are documented in the Upgrading to X7.2 section of this document.

After upgrading to X7.2

Note the following important configuration information, following an upgrade to X7.2:

- The default Traversal Subzone media port range is now 50000 - 54999 (previously 50000 - 52399), in order to support the new media encryption policy feature. To reflect this change, system administrators may need to modify the rules configured in their firewall devices.
- Core dump mode is enabled (even if it was previously disabled). It can be configured on the **Incident reporting configuration** page.
- An “Insecure password in use” alarm will be raised against the root account. This is because the VCS now uses SHA512 to hash passwords. Passwords were previously hashed using MD5. The root account will still be accessible but you are recommended to use the root passwd command to reset the root account password. Administrator account passwords are rehashed automatically on upgrade.
- If the system was previously configured to use *Remote* authentication as its **Administrator authentication source** this will be changed to the new *Both* option which allows both locally and remotely maintained administrator accounts to log in to the VCS, and any pre-existing local administrator accounts will be set as *Disabled*.

- If you subsequently downgrade from X7.2 to X7.1 all local administrator accounts will have their passwords reset to TANDBERG.

TMS Provisioning Extension mode

You must upgrade your VCS or VCS cluster (while still in TMS Agent legacy mode) to X7.1 or X7.2, before installing TMS Provisioning Extension (TMSPE) and switching TMS and VCS into Provisioning Extension mode.

You are recommended to switch to TMS Provisioning Extension (TMSPE) mode, if you are using Cisco TMS with Provisioning or FindMe, when the upgrade to X7.2 is complete and proven to be operating correctly.

To switch to Provisioning Extension mode (from TMS Agent legacy mode), you must upgrade TMS to TMS 13.2 or later. See *Cisco TMS Provisioning Extension Installation Guide*.

Upgrading a non-clustered VCS to X7.n from X5.1, X5.1.1 or X5.2

If you are currently running VCS X5.1, X5.1.1 or X5.2, you must first upgrade to X6.1, then upgrade from X6.1 to X7.n.

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

If you are currently running VCS X5.0 or earlier, you must first upgrade to X5.2, then upgrade from X5.2 to X6.1, and then upgrade from X6.1 to X7.n.

Device authentication

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

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

Cisco VCS upgrades where authentication is not enabled

If device authentication is not enabled when the Cisco VCS is upgraded from X5.2 or earlier to X7.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 in TMS Agent Legacy mode)

If you are upgrading from X6.n to X7.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 upgrades where authentication is already enabled

If device authentication is enabled when the Cisco VCS is upgraded from X5.2 or earlier to X7.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 (if in TMS Agent Legacy mode)

TMS Provisioning Extension mode / Cisco VCS Starter Pack Express

When TMS and VCS are running in Provisioning Extension mode, or you are running a Cisco VCS Starter Pack Express, the VCS's Provisioning Server requires that any provisioning or phone book requests it receives have already been authenticated (the Provisioning Server does not do its own authentication challenge):

- You must ensure that the Default Zone and any traversal client zone's **Authentication policy** is set to either *Check credentials* or *Treat as authenticated*, otherwise provisioning requests will fail.
- The authentication of phone book requests is controlled by the **Authentication policy** setting on the Default Subzone (or relevant alternative subzone) if the endpoint is registered (which is the usual case), or by the **Authentication policy** setting on the Default Zone if the endpoint is not registered. The relevant **Authentication policy** must be set to either *Check credentials* or *Treat as authenticated*, otherwise phone book requests will fail.

Presence and device authentication

The VCS's Presence Server only accepts presence PUBLISH messages if they have already been authenticated (the Presence Server does not do its own authentication challenge):

- The authentication of presence messages by the VCS is controlled by the **Authentication policy** setting on the Default Subzone (or relevant alternative subzone) if the endpoint is registered (which is the usual case), or by the **Authentication policy** setting on the Default Zone if the endpoint is not registered. The relevant **Authentication policy** must be set to either *Check credentials* or *Treat as authenticated*, otherwise PUBLISH messages will fail.

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

Hierarchical dial plan (directory VCS) deployments

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

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

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

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

message will be identified as coming through that neighbor zone, the VCS will not perform any credential checking (as the neighbour zone is set to *Do not check credentials*) and the message will be accepted.

Deployments with multiple regional / subnetwork directory VCSs

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

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

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

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

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

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

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 X7.2 "Cluster Creation and Maintenance" Cisco VCS deployment guide, or by following the "Upgrading to X7.2" instructions in this document.

New features in X7

X7.2.2

This is a maintenance release.

X7.2.1

This is a maintenance release.

- The VCS Starter Pack Express supports Cisco Jabber for iPad.

This release also contains some third-party software updates: Python has been upgraded to 2.7.3, PHP has been upgraded to 5.3.15, and TLS 1.1 and 1.2 have been enabled in Apache.

X7.2

Controlled SIP TLS connections to the Default Zone

Default Zone access rules that control which external systems are allowed to connect over SIP TLS to the VCS via the Default Zone can now be configured.

Each rule specifies a pattern type and string that is compared to the identities (Subject Common Name and any Subject Alternative Names) contained within the certificate presented by the external system. You can then allow or deny access to systems whose certificates match the specified pattern.

Enabling this feature requires that all systems (including endpoints) connecting to the Default Zone must present client certificates that are trusted by the VCS.

Device authentication

- The VCS can now be configured to authenticate devices against multiple remote H.350 directory servers. This provides a redundancy mechanism in the event of reachability problems to an H.350 directory server.
- As from version X7.2, for Digest authentication, the VCS attempts to verify device credentials presented to it by first checking against its on-box local database of usernames and passwords, before checking against any configured H.350 directory server. (Note that the endpoint presents the VCS with a the hash of its credentials, which the VCS attempts to validate against a hash created from the credentials stored in the local database - the VCS does not see the actual credentials from the device.) As a result of this:
  - The **Device authentication configuration** page no longer exists; there is no longer an option to switch between an authentication database type of *Local database* or *LDAP database*.
  - The **NTLM protocol challenges** setting is now configured on the **Active Directory Service** page.
- The **Device LDAP configuration** and **Device LDAP schemas** pages are now called **Device authentication H.350 configuration** and **Device authentication H.350 schemas** respectively.
- The **Alias origin** field on the **Device authentication H.350 configuration** page is now called **Source of aliases for registration**.

Enhanced account security

- Administrator accounts can now be configured to authenticate first against the local database and then if no matching account is found to fall back to a check against the external credentials directory.
- When defining administrator accounts and groups, you can now also specify if the account/group can access the web interface and/or the XML/REST APIs.
- When strict passwords are enforced for administrator accounts, you can now customize the rules for what constitutes a strict password.
- Local administrator passwords are now stored using a SHA512 hash.
- In a cluster, the default admin account password is now replicated across all peers.
- Note that the "Login Administrator" set of xConfiguration CLI commands are no longer supported.

System security enhancements

- You can now configure firewall rules to control access to the VCS at the IP level. You can:
  - specify the source IP address subnet from which to allow or deny traffic
  - configure well known services such as SSH, HTTP/HTTPS or specify customized rules based on transport protocols and port ranges
- The VCS can be configured to use a combination of OCSP and CRL checking for certificates exchanged during SIP TLS connection establishment. CRLs can be loaded manually onto the VCS, downloaded automatically from preconfigured URIs, or downloaded automatically from a CRL distribution point (CDP).
- The VCS can now generate server certificate signing requests. This removes the need to use an external mechanism to generate and obtain certificate requests. The upload of the VCS's trusted CA certificate and the management of its server certificate are now configured on separate pages under the **Maintenance > Certificate management** menu.
- When enabling client certificate-based security you can now configure CRL checking behavior.
- VCS can now be configured to use HTTP Strict Transport Security (HSTS). This can be used to force a web browser to communicate with the VCS using secure connections only.
- Access to the VCS via the serial port can be disabled.
- You can configure the authentication method used by the VCS when connecting to an NTP server. It utilizes the security features available in NTPv4 and retains compatibility with NTPv3 implementations. Options include symmetric key message hashing and private key encryption.
- System backup files can now be encrypted / password protected. (Note that encrypted backup files normally have a ".tar.gz.enc" filename extension. However, if you use Internet Explorer to create an encrypted backup file, the filename extension will be ".tar.gz.gz" by default. These different filename extensions have no operational impact; you can create and restore encrypted backup files using any supported browser.)
- OpenSSL has been updated to version 1.0.1 (includes support for TLS v1.2).

Zone and subzone media encryption policy

Media encryption policy settings allow you to selectively add or remove media encryption capabilities for SIP calls flowing through the VCS. This allows you to configure your system so that, for example, all traffic arriving or leaving a VCS Expressway from the public internet is encrypted, but is unencrypted when in your private network. The policy is configured on a per zone/subzone basis; this level of granularity means that different encryption policies could be applied to each leg of a call in/out of a zone/subzone.

Call processing

When configuring search rules you can now specify:

- The source protocol for which the rule applies.
- A specific source zone or subzone for which the rule applies. Named sources creates the ability for search rules to be applied as dial plan policy for specific subzones and zones.

Improved interworking flow control

The VCS now supports the ability to interwork the H.323 flowControlCommand into RFC 5104 Temporary Maximum Media Stream Bit Rate Request (TMMBR). This provides the ability to stem the flow of data from a remote participant.

Enhanced diagnostics

- There is an improved filter mechanism for call and registration status management.
- Search history shows additional information including search start timestamps and durations, and improved reporting of search failure reasons.
- A Tracepath network utility has been added (to complement the existing traceroute tool).
- The Locate tool now allows you to specify a specific subzone (or zone) as the source of the search request.
- The VCS now supports IETF format messages when sending events to remote syslog servers. Note that the **Logging** page is now located under the **Maintenance** menu.
- When a diagnostic log file is downloaded, the filename now includes the local host name; this helps distinguish it from diagnostic files downloaded from other cluster peers.
- Core dump mode is now enabled by default. It can be configured on the **Incident reporting configuration** page; it can no longer be configured via the CLI.
- System snapshot files now include a list of active alarms.

Other enhancements and usability improvements

- The default Traversal Subzone media port range is now 50000 - 54999 (previously 50000 - 52399), in order to support the new media encryption policy feature. To reflect this change, system administrators may need to modify the rules configured in their firewall devices.
- Up to 20 policy services can now be configured (the limit was 5 previously).
- When configuring a DNS zone you can now specify a **TLS verify subject name** to use when verifying the destination system server's certificate.
- The %ip% pattern matching variables now apply to all peer addresses if the VCS is part of a cluster; when used in a replace string the variable is always substituted with the address of the local peer only.
- The Microsoft B2BUA now supports up to 100 simultaneous calls (the limit was 50 previously); however, calls that use transcoder resources count as 2 calls.
- TURN server now has full IPv6 support (as per RFC 6156). The **TURN relays status** page displays the addresses on which the TURN server is listening, and the addresses from which it is allocating relays.
- The VCS now supports early dialog SIP UPDATE messages. Note that the relevant zone must be configured with **SIP UPDATE strip mode** set to *Off* (set via the *Custom* zone profile).
- Automatic CRL updates can now use HTTPS distribution points.
- DNS queries can now be configured to use the ephemeral port range or to use a customized range.
- The **Clustering** page displays the name (in addition to the address) of all of the peers.
- The SIP **Domains** page includes an **Index** column that corresponds to the numeric elements of the %localdomain1%,%localdomain2%, . . . %localdomain200% pattern matching variables.
- When upgrading software components, the MD5 and SHA1 hash values of the software image file being uploaded are displayed for user verification (when upgrading from X7.2 or later).

- There is no longer a need to restart the VCS after uploading a language pack.

Support for some xConfiguration commands removed

The following xConfiguration CLI command sets are no longer supported:

- xConfiguration Administration HTTPS RequireClientCertificate
- xConfiguration Administration MaxConcurrentSessions
- xConfiguration Administration TimeOut
- xConfiguration Authentication Database
- xConfiguration Authentication LDAP BaseDN
- xConfiguration Certification AdvancedAccountSecurity
- xConfiguration Core Dump Mode
- xConfiguration Error Reports
- xConfiguration IP DNS Server
- xConfiguration LDAP
- xConfiguration Log
- xConfiguration Login Administrator
- xConfiguration Login User
- xConfiguration NTP Address
- xConfiguration SNMP
- xConfiguration SystemUnit AdminAccount
- xConfiguration SystemUnit Password
- xConfiguration SystemUnit StrictPassword
- xConfiguration TimeZone Name

X7.1

TMS Provisioning Extension support

VCS X7.1 supports the Provisioning Extension mode introduced into Cisco TMS v13.2.

In X7.0 and earlier, the provisioning, FindMe and phonebook services on the VCS were provided by the legacy TMS Agent module. From X7.1, the new Provisioning Extension services mechanism supports large-scale deployments and provides a more flexible upgrade path for both VCS and Cisco TMS.

You are recommended to switch from using the TMS Agent legacy mode to the new Provisioning Extension mode as soon as is practicable.

Call processing

- Improved interworking between VCS and Cisco Unified Communications Manager (CUCM). VCS now always stays in the call signaling route for calls to neighbor zones that are configured with the Cisco Unified Communications Manager or the Infrastructure device zone profiles.

Virtual appliance support

- The VCS can run on VMware on Cisco UCS C200 M2, UCS C210 M2, or UCS B200 M2 servers.
- See *Cisco VCS Virtual Machine Deployment Guide* for installation instructions.

Other enhancements and usability improvements

- Improved status reporting of NTP server synchronization.
- The lower and upper source ports in the range used for sending DNS queries can now be configured on the DNS page.
- Automatically uploaded CRL files are now included when checking the validity of client certificates on the Client certificate testing page.
- System snapshot:
  - The snapshot process now runs in the background. This means you can navigate away from the snapshot page and return to it later to download the generated snapshot file.
  - Snapshot filenames are distinct for each type of snapshot.
- Default incident reporting server is now https://cc-reports.cisco.com/submitapplicationerror/
- The VCS Starter Pack Express supports device provisioning for MX200 endpoints.
- An optional free-form description of a B2BUA transcoder can be specified.
- Alarms status page now shows when an alarm was first raised.
- The VCS web interface now supports Internet Explorer 7, 8 or 9, Firefox 3 or later, or Chrome. Later versions of these browsers may also work, but are not officially supported.
- The VCS now uses syslog-ng for logging; if syslog-ng log entries are seen these are typically recording rotating log files.

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.
- Reverse Path Filtering (RFC1812) is enabled by default. This ensures that the VCS will only accept packets on interfaces from source addresses to which there are valid routes in the routing table for that interface. This change may necessitate the adding of additional static routes on dual-interface VCSs to ensure the VCS routing table matches the network topology.

Resolved caveats

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

Resolved in X7.2.2

Identifier	Summary
CSCue41065	**Symptoms**: Data loss on upgrades, typically X7.1 -> X7.2.1. Typically lost data is NTP, DNS, Admin Accounts, TimeZone, and all but two Option Keys. **Conditions**: Upgrading to X7.2.1. **Workaround**: Reboot into the previous image, and try the upgrade again.
CSCue41164	**Symptoms**: Time synchronization problems and the raising of NTP server-related alarms. **Conditions**: Only applies when running as a Virtual Machine. **Workaround**: Configure the VMware host and the VCS with the same NTP server.
CSCub63112	**Symptoms**: Calls to TelePresence Conductor fail. Error message on the Conductor policy service page on the VCS is: "Failed: SSL connect error. Last connection attempt: 2012-06-11 14:38:04 " **Conditions**: Non AES VCS attempting to communicate with a Conductor **Workaround**: None.
CSCub42318	**Symptoms**: A VCS will see slowly climbing memory usage, eventually seeing the swap partition be used and performance drop, and occasionally crashes due to delayed database access. **Conditions**: This only affects clustered VCSs that are doing millions of searches. **Workaround**: Monitor memory usage by doing the following as root: cat /proc/meminfo | grep Committed_AS If usage exceeds 4.5GB, the VCS should be rebooted.
CSCuc13370	**Symptoms**: Event Log does not respect the value set under Maintenance > Logging > Log Level on the web in X7.2. It always defaults to level 1, the least verbose. This means when selecting "View all events associated with this call" hyperlink for a call, less detail is displayed than expected. **Conditions**: Seen with Cisco VCS running X7.2. X7.1 and previous versions of VCS software are not affected by this issue. **Workaround**: None.
CSCuc40064	**Symptom**: VCS B2BUA does not advertise the maximum bit rate correctly for CIF and QCIF. When CIF (2500) and QCIF (1800) are being signaled, the maxbr is set to 1800 (meaning the ability to receive 250 kbps for CIF has disappeared). **Conditions**: VCS B2BUA in use for Lync integration. **Workaround**: None.
CSCuc75149	**Symptoms**: Call from Lync to Polycom HDX registered on H323 fails. **Conditions**: In the case of a Lync to H323 call, the SimultaneousCapabilities in the TCS do not match provided capability in the table, leading to the call failing to a Polycom HDX endpoint. **Workaround**: None, however calls from HDX to Lync work as expected. **Additional information**: This is caused by incorrect entries in the AlternativeCapabilitySet in the TerminalCapabilitySet sent by the VCS.
CSCuc98344	**Symptoms**: The Subzones page on VCS does not show all subzones, and is missing all buttons on the lower part of the page. **Conditions**: This can be seen if the VCS has a high number of subzones combined with a high number of calls and/or registrations associated with these subzones. In addition, the Apache error.log file may show entries similar to: PHP Fatal error: Maximum execution time of 30 seconds exceeded in /share/web/lib/statusadaptationlayer.php on line 199

Identifier	Summary
	Workaround: None.
CSCud16570	**Symptoms**: A crash report may be seen on the VCS: "An unexpected software error was detected in ivy[1748]: SIGABRT (tkill(2) or tgkill(2))" **Conditions**: A crash with this signature can occur when an Advanced Media Gateway is in use with a VCS communicating with Microsoft Lync, and there is another box in the call that alters the Call-ID after the call has been forked by the VCS. **Workaround**: Remove the call fork.
CSCud20001	**Symptom**: X7.2.1 VCS publishes wrong presence status on behalf of registered HDX/VSX. The end result is that the HDX and VSX endpoints will be shown with "offline" instead of "online" (SIP). When subscribing for presence status, the notify is returned with closed status: <?xml version='1.0' encoding='UTF-8'?><presence><tuple><status><basic>closed</basic></status></tuple></presence>| **Conditions**: Subscribed for presence from registered HDX and VSX. Default published status for registered endpoints is set to Online on VCS. **Workaround**: None.
CSCud62567	**Symptoms**: An upgrade of a Cisco VCS with local FindMe accounts will lose these accounts on an upgrade to X7.1 or later. **Conditions**: This will occur if the usernames contain non-ASCII characters. **Workaround**: Rename the affected users.
CSCud89476	**Symptoms**: Incident report generated: ACR: b2bbridgecontextevent Line: 339. Calls to and from MS Lync via the Microsoft OCS/Lync B2BUA process drop/fail to connect. **Conditions**: Calls routed via the Microsoft OCS/Lync B2BUA process. **Workaround**: The Microsoft OCS/Lync B2BUA process is automatically restarted.
CSCud50912	**Symptoms**: Some H.323 calls hang on the VCS. Rebooting the VCS will clear the calls but the point at which the calls are cleared without a reboot can affect TMS call reporting. **Conditions**: Issue has been seen when H.323 call setup does not complete properly and the VCS returns release complete to call initiator but does not free up its internal call information. **Workaround**: None.
CSCub76176	**Symptoms**: Calls from unregistered endpoints, behind a NAT, into a VCS Expressway may be dropped at 15 minutes. **Conditions**: SIP Session Refresh when set to 1800 seconds or greater (where it will refresh after approximately 900 seconds) will fail if the unregistered endpoint is behind a NAT, and so the VCS Expressway cannot connect back to it in order to refresh the session, after the initial TCP session has been torn down. **Workaround**: Set the SIP Session Refresh (VCS configuration > Protocols > SIP > Configuration) to be less than 1800 seconds, for example 1200 seconds (so it will refresh after approximately 600 seconds).

Resolved in X7.2.1

Identifier	Summary
CSCub34963	**Symptoms**: On upgrade to X7.2, local users or members of a remote (Active Directory) group may not be able to log in on the web interface of the VCS. **Conditions**: If a remote administrator group and a local admin user have the same name, only one will be permitted access to the VCS web interface. **Workaround**: Rename the remote group or the local user. Access to the VCS will still be permitted by one or the other way.
CSCub66229	**Symptom**: TMS will not produce CDR data of type "Gatekeeper and VCS", and the log-web-public.txt log file in TMS will contain entries similar to: ---> Tandberg.TMS.SystemAPI.OakPine.InvalidStateException: Expected to find <Legs>, but instead found <EndTime>. at Tandberg.TMS.SystemAPI.OakPine.XMLFeedbackReader.AssumePositionedAtTag (XmlReader reader, String tag)

Identifier	Summary
	at Tandberg.TMS.SystemAPI.OakPine.XMLFeedbackReader.ProcessCall(XmlReader reader) at Tandberg.TMS.SystemAPI.OakPine.HttpFeedback.ProcessCallDisconnected(IXMLDoc txasDoc, RoutableSystem system) --- End of inner exception stack trace --- TMS Version 13.2.1 **Background**: Because of a change in the XML feedback which the VCS sends to TMS for events related to calls connecting and disconnecting, TMS is not able to properly interpret the XML data provided by the VCS. Because of this, TMS is not able to generate CDR records based on the feedback data provided by the VCS. **Workaround**: There is currently no known workaround for this issue when running X7.2 software on the VCS. X7.1 and previous versions of VCS software are not affected by this issue.
CSCub31927	**Symptom**: Attempting to use Cisco Jabber for iPad with a Cisco VCS Starter Pack Express results in the Jabber client not being able to register to the VCS Expressway. **Conditions**: Must be attempting to register the Cisco Jabber for iPad to a Cisco VCS Starter Pack Express with no Cisco TMS in play. Cisco Jabber for iPad tries to register with device type "jabbertablet" which is unknown. **Workaround**: No workaround available. Customer must deploy Cisco TMS solution in order to user Cisco Jabber for iPad client.
CSCuc16057	**Symptom**: Some older versions of Polycom endpoints registered on VCS failed to establish call after software upgrade to X7.2. **Conditions**: The VCS strips/filters some terminalCapabilitySet items based on the vendor and H.323 version. However, with X7.2 these terminalCapabilitySet messages sent to the Polycom ViewStation are larger than it can cope with (capability related to H.239). The Polycom ViewStation stops responding to call negotiation from VCS after the terminalCapabilitySet message and the call terminates by call setup timeout on endpoint. **Workaround**: Disable H.239 on calling device (far end endpoint, MCU, etc.).
CSCub25632	**Symptom**: When using the VCS B2BUA, an MCU joining a conference may not be aware it is an MCU and will join as a regular participant. **Conditions**: This only occurs when the VCS B2BUA is in use to enforce encryption policy on the participating call legs. **Workaround**: Do not use the VCS B2BUA in these circumstances and instead manually verify participant encryption status.
CSCub68929	**Symptoms**: When a 9971 phone dials into a Cisco TelePresence Server meeting and does a hold/resume for the second time, you get a black screen. The first hold/resume works fine (you get video after resume), but any further hold/resumes result in a black screen.
CSCua49125	**Symptoms**: When the VCS sends a SIP INVITE, the P-Asserted-Identity field does not contain a display name. This results in no caller ID on the far end. Currently the PAI header will look like this: P-Asserted-Identity: <sip:name.ex60@ name.local> Instead, it should look like this: P-Asserted-Identity: "Full Name" <sip: name.ex60@ name.local> **Conditions**: When VCS sends an invite to CUCM (or other 3rd party SIP server), the P-Asserted-Identity field does not contain a display name while VCS run X7.2 or older software version.
CSCua80573	**Symptoms**: Logins on the web and CLI can be slow to complete. **Conditions**: When remote authentication is enabled, all logins (not just remote users) can be delayed by many seconds if the LDAP server is slow to respond. **Workaround**: None, delays from the LDAP server are outside the control of the VCS.
CSCub89101	**Symptoms**: A crash report is seen on the VCS for the "python" application, with statements such as "unable to read python frame information". **Workaround**: None, however Python processes on the VCS will immediately restart and this should not disrupt service.
CSCub18559	**Symptoms**: The hard disk on a VCS can become full if the log rotation program fails. This can lead to unexpected errors such as database and web access issues.

Identifier	Summary
	Conditions: This will occur if the log rotation program fails, and the log files grow to fill up /var/log. **Workaround**: Delete the non-rotated log files in /var/log, or move them out of the way to /mnt/harddisk.
CSCud24211	**Symptom**: Cisco TelePresence Video Communication Server (VCS) may report an early fan "Hardware Failure" alarm condition that does not impact the server. **Condition**: A VCS running a release prior to X7.2.1 will report a hardware failure alarm if a single fan reports a speed below 7670 RPMs. The impact of this threshold is that fan fluctuations that do not impact the functionality of the server have led to units being prematurely replaced. Starting in X7.2.1, new alarms values based upon extensive testing have been implemented. **Workaround**: For systems running with releases prior to X7.2.1, you can safely ignore the alarm if the VCS displays only one fan alarm message for a single fan. Customers should monitor such alarms manually. The VCS includes temperature alarms that are raised if the VCS reaches an unsafe temperature. **Additional Information**: You can log in to the VCS as root and run the "sensors" command to get more detailed information on system fans and temperature.

Resolved in X7.2

Identifier	Summary
CSCty97265	**Symptoms**: A H323/SIP interworked G729 audio call may drop after the first session refresh. **Conditions**: Offer/answer in H323/SIP interworked case may not send G729 capability in SDP re-invite (at session refresh) since G729 can be signaled multiple times in H323 but only once in SDP. **Workaround**: Use SIP only.
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.
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.
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.
CSCts25426	**B2BUA 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.
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(.*)

Identifier	Summary
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 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.
CSCtw75336	**Symptoms**: On dual network interface VCS, if the default gateway is in LAN 2's subnet, VCS User Interface will show the gateway address as 127.0.0.1 **Conditions**: Dual network interfaces on VCS and default gateway in LAN 2 subnet **Workaround**: Not a critical problem - this is a display only problem
CSCtx15355	**Symptom**: When receiving a H.323 Setup message and interworking it on the Cisco VCS, the SIP INVITE may go out with Contact and From headers of iwf@VCS_IP_Address if there is no Calling Party Number details in the H323-UserInformation section - VCS interworking should in that case take the calling party ID from other source information in the H.323 message, e.g.Q931 Calling Party Number digits. **Conditions**: None. **Workaround**: None.
CSCtz43853	**Symptoms**: OCS/Lync responds with '405 Method not allowed' for a SIP INFO request sent from VCS (via B2BUA if in use) for an interworked (H323 > SIP) call. **Conditions**: A '405 Method not allowed' response may be seen from OCS/Lync in response to a SIP INFO sent from VCS (via B2BUA when in use) when a third-party SIP application/service exists within the OCS/Lync environment, and this service does not support the SIP INFO method which the VCS uses in its interworking search strategy. The 'Server' header of the 405 response message will identify this third-party SIP application/service, for instance: "Server: RTCC/3.5.0.0 BPOCSMobileStatus/1.4.1.115". **Workaround**: The workaround (for X7.1 and earlier) is to change the zone profile for the OCS/Lync neighbor zone (Or the "To Microsoft OCS/Lync server via B2BUA" zone for B2BUA deployments) to 'Custom' and set the "Automatically respond to SIP searches" setting to 'On'. Changing the zone profile for the "To Microsoft OCS/Lync server via B2BUA" zone has to be done from the VCS CLI using the command 'xconfiguration Zones zone 1 Neighbor ZoneProfile: Custom', where '1' denotes the corresponding zone number for the "To Microsoft OCS/Lync server via B2BUA" neighbor zone". Note that the zone profile should be set back to its default value of "LocalB2BUAService" before the VCS is upgraded to X7.2, using the command "xconfiguration Zones zone 1 Neighbor ZoneProfile: LocalB2BUAService" (Still assuming that zone 1 is the corresponding B2BUA neighbor zone), as this limitation will be addressed in X7.2. **Additional Information**: In X7.1 and earlier, the VCS will only interwork calls from H323 to SIP when the OPTIONS/INFO SIP search for the interworked call is responded to with "481 Call/Transaction does not exist". In X7.2 and later, a "405 Method now allowed" response will also be counted as a valid interworking response.
CSCty38860	**Symptoms**: In X7.1 and prior the VCS NTLM AD setup page status does not report the correct status - it often reports Joined, when a root level net ads testjoin reports that really the VCS is not joined to the domain. **Conditions**: This occurs if the VCS has lost its binding with Active Directory, possibly by losing sync of password changes or the account becoming disabled. **Workaround**: Rejoin the domain.
CSCtx54656	**Symptoms**: The VCS webserver becomes unresponsive, but the rest of the VCS functionality is unaffected. Various "web: [error] [client xxx.xxx.xxx.xxx]" logs messages may be seen. **Conditions**: This was seen on a Cisco VCS running X7.0.2. **Workaround**:If the VCS gets into this state, restart the VCS
CSCua81088	**Symptoms**: A client may report a VCS having an incomplete certificate chain.

Identifier	Summary
	Conditions: If the VCS's certificate is signed by a CA's intermediate certificate and the client does not have the intermediate certificate installed, the certificate may be reported as invalid. **Workaround**: Install the intermediate certificate on a client PC. **Additional information**: The full certificate chain is provided by Apache in X7.2. This does not affect the TLS-encrypted SIP, which always provides the full certificate chain.
CSCtx86755	**Symptom**: Scrolling of data tables in web interface is inconsistent between browsers. IE8 - No table scrolling IE9 - table headings are hidden when scrolling IE8 and IE9 (compatibility mode) - Distorted column headings Chrome - No table scrolling Firefox 7 - No table scrolling Safari - No table scrolling **Workaround**: Do not use "Compatibility View" mode in IE.
CSCua49148	**Symptoms**: In an interworked call (SIP <> H323), the H323 device involved in the call might experience no incoming video if a SIP INFO request which is interworked from an H323 Fast Update Request is challenged for credentials. **Conditions**: No video is seen on the H323 device if a SIP INFO request interworked from an H323 Fast Update Request is challenged for credentials. **Workaround**: Register the H323 device in SIP and ensure that the call uses SIP throughout rather than interwork to H323.
CSCty98383	**Symptom**: Far end camera control is not available when calling from Cisco IP video phone E20 -> sip -> CUCM -> sip -> VCS -> h.323 -> MCU 5300 **Condition**: The problem was observed with Cisco IP Video Phone E20 running TE 4.1.1 **Workaround**: No workaround available.
CSCty19138	**Symptoms**: Cluster replication fails and the following warning is raised: "Cluster replication error: this peer's configuration conflicts with the master's configuration, manual synchronization of configuration is required" **Troubleshooting**: This generates three files in /tmp/ on the peer: config_MASTER_IP.xml config_PEER_IP.xml config_diff_MASTER_IP_PEER_IP.xml The two config files should be the same they contain all the configuration that is replicated from the master to the peer. In this case they are not. The config_diff shows the differences between the two. In the case of this issue the difference is the result of the Access level being different. The diff file should show the line in tsh where the difference occurs. Access item="1" in the diff corresponds to xconfiguration SystemUnit AdminAccount 1 Access: **Workaround**: For each AdminAccount in tsh where there are discrepancies between the master and slave peer names, on the master peer enter via the CLI: xconfiguration SystemUnit AdminAccount 1 Name: NAME xconfiguration SystemUnit AdminAccount 1 Access: ReadWrite These should then be synchronized successfully with the slave peer. The account can then be removed. Setting the access level to its default (ReadWrite) prevents the issue occurring again when new peers are added to the cluster.
CSCty35457	**Symptom**: VCS 'Infrastructure device' neighbor zone reports DNS resolution failed even though DNS lookup is OK. Calls through that zone fail. **Conditions:** If a DNS problem occurs the zone goes down and does not subsequently recover. **Workaround**: Specify an IP address rather than a DNS name.
CSCty29175	**Symptom**: SIP - H.323 interworked calls may appear hung in Connecting state in the Cisco VCS web UI and also show failure reason information : Reason: Gatekeeper resources

Identifier	Summary
	Cause: Temporary failure Additional cause: Out of call resources When the target alias of the call includes the Cisco VCS IP address. **Conditions**: This was seen on a Cisco VCS running X7.0.3. **Workaround**: Restarting the Cisco VCS will clear the hung call from the UI.
CSCub20678	**Symptoms**: Although cluster connectivity is Active, not all cluster peers are shown on the Overview page. Inconsistencies in cluster alarms may also occur. **Conditions**: This can occur in a cluster of 3 or more peers, where not all peers are rebooted, and when the peers return they do not properly rejoin the cluster. **Workaround**: Reboot all cluster nodes at the same time.
CSCty33261	**Symptom**: Customers cannot log in to either the web interface or SSH as admin . **Conditions**: VCS X7.0.1 with Open-DS installed. **Workaround**: The issue is resolvable by running tmsgent_destroy_and_purge_data and rebooting. As the command name says, this will purge and destroy data. Only run this command under the guidance of TAC - and see notes in VCS Cluster deployment guide. You will destroy data so if it is not saved elsewhere it will be lost forever
CSCty45249	**Symptom**: Provisioning failure for users on 2nd cluster registering to shared Expressway. Users on Cluster 2 cannot log in to Movi on the Expressway, the error message “Did not receive provisioning in time” is seen on Movi. This is because Cluster 1 sends a 200 OK to the SUBSCRIBE for provisioning for the user even though the user does not exist on Cluster 1. It then sends a rejection NOTIFY message, but provisioning is then not tried on Cluster 2. **Conditions**: Seen on VCS X7.1 when there are two VCS Control clusters sharing one VCS Expressway cluster **Workaround**: Put in specific rules so that provisioning requests for users on Cluster 2 are only sent to Cluster 2 from the VCS Expressway, and not tried on Cluster 1 first.
CSCty46071	**Symptom**: The VCS application can crash with an error in "fillCapabilityTable" during interworking. **Conditions**: This can occur if an incoming SDP message contains certain encrypted special capabilities that cannot be cleanly mapped to a H323 TerminalCapabilitySet. **Workaround**: This bug has yet to be seen in a repeatable nature, so it is unclear if there are other workarounds. **Additional Information**: The underlying issue in the VCS has been fixed.
CSCty91599	**Symptom**: If VCS interworking is being used on both ends of a H.323 neighboring, such as a scenario involving an IPVCR: UCM -(SIP)- VCS -(H323)- IPVCR -(H323)- VCS -(SIP)- UCM, a call may not be established. **Conditions**: The VCS will wait 30 seconds before sending a Terminal Capability Set over the H.323 link, expecting to receive one first. This is longer than the 20 second timeout seen on the Cisco UCM as a SIP peer. **Workaround**: None available.
CSCty93624	**Symptom**: Licenses may be allocated to calls that were never set up. **Conditions**: This can occur if the database is taking too long to respond, and the license is eventually allocated after the caller has timed out trying to set up the call. **Workaround**: These allocated licenses can be cleared by restarting the VCS.
CSCty97430	**Symptoms**: Calls and other SIP traffic failing. Lync servers not able to communicate with B2BUA. **Conditions**: This can be seen if B2BUA has used up all 20 TCP connections for SIP traffic. To check the current number of active TCP connections in use by the B2BUA, run the command 'netstat -anp | grep ESTABLISHED | grep /ivy | grep -v :127.0.0.1:4370' from a root SSH shell on the B2BUA VCS. **Workaround**: Reduce the number of Lync hosts communicating with B2BUA, for example by routing all Lync to VCS traffic through a single Director server. **Additional Information**: None.
CSCtz35304	**Scenario**: An H.323 MCU contains a SIP endpoint in the conference. If the SIP endpoint gets its network connection disconnected, a frozen picture remains forever on the conference.

Identifier	Summary
	Conditions: A SIP/H.323 interworked call is never torn down at the H.323 end despite 408 Request Timeout messages being generated. **Workaround**: None, although non-interworked calls will not be affected.
CSCua02807	**Symptoms**: The VCS loses its connection to Active Directory (identified by running "net ads testjoin" on the root command line) and users cannot be authenticated with NTLM. **Conditions**: This will occur if an AD server does not respond to a machine account password change request within 10 seconds. **Workaround**: Re-join the domain with the "domain_management" command as root. A fix to disable machine password refreshes will be developed. **Additional info**: Note that the NTLM web page does not show the correct join status in this scenario. This is addressed by CSCty38860.
CSCua11868	**Symptom**: When calling from VCS to OCS/Lync via B2BUA, B2BUA removes ";user=phone" from the request-URI. **Conditions**: None. **Workaround**: None.
CSCud58380	**Symptom**: Security Issue in Apache. Vulnerabilities CVE-2012-0883, CVE 2012-0053, CVE 2012-0031, and CVE 2012-0021 apply to Apache version 2.2.21 found in Cisco VCS version X7.1. **Conditions**: None. **Workaround**: Upgrade to Cisco VCS X7.2.x **Additional Information**: Cisco VCS version X7.2.x runs Apache version 2.4.2 which resolves these issues.

Resolved in X7.1

Identifier	Summary
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.
CSCtx34916	Duplicate of CSCtx34918.
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.
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'
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.
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.
CSCtx71406	**Symptoms**: Make an interworked call from an H.323 MCU 4.3 to Movi and send some content to Movi. Then from the participants list page disable content to Movi. Movi continues to display content but the content freezes at the point of disabling.

Identifier	Summary
	If instead of disabling content via the MCU web interface, you actually stop sending content from the endpoint, then Movi stops showing content correctly. Both cases work when using an interworked E20 instead of Movi though. **Conditions**: MCU 4.3 H.323 Movi. **Workaround**: None.
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 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
CSCtw53707	The VCS contains an experimental section that is disabled by default but can be enabled if one knows the password. It is a violation of the Product Security Baseline to have hidden commands. This experimental interface should either be enabled for everyone or removed entirely. The Experimental menu is now documented in the VCS online help and Administrator Guide.
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.
CSCtx20426	Duplicate of CSCtx24759.
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.
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.
CSCts25438	**B2BUA does not disconnect a call on 408 (Request Timeout) responses**: B2BUA does not disconnect a call when it receives a 408 response to a fast update request. The call remains visible under call status and if the Cisco VCS Expressway is used for TURN services the TURN session will remain.
CSCtx34833	**Symptoms**: Incident report raised 'Reason: Detail="Failed to notify file system observer". **Conditions**: None. **Workaround**: None. **Additional Information**: XML Parse exceptions should re-try rather than produce Incident Report.
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-master peer in turn to activate the account. Make sure the non-master peer has completed its restart before restarting another peer.

Identifier	Summary
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
CSCtx34918	**Symptoms**: Incident report or alarm raised for Linux updates failing, e.g. Application failed An unexpected software error was detected in managementframework.py: Detail="Failed to update linux status" **Conditions**: None. **Workaround**: None.
CSCtt47470	**Symptom**: NTLM Enhanced Session security not currently supported. **Conditions**: All VCS code prior to X7.1. **Workaround**: None. **Additional Information**: Enhanced Session security support added in VCS X7.1.
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.
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.
CSCty97645	**Symptoms**: VCS runs out of sockets if TLS handshake fails - VCS fails to clean up sockets on certain handshake failures. **Conditions**: None. **Workaround**: None.
CSCtx34719	**Symptoms**: Incident report "(ClusterDB:cm_server.erl:gen_server:call/2:Unknown)V:X7.0.2N:s42700" or "(ClusterDB:clusterdb_module_ntpServerStatus.erl:gen_server:terminate/6:Unknown)" raised **Conditions**: None. **Workaround**: None. **Additional Information**: Caused by high disk i/o - fixed by using a write through cache on the disk.
CSCtx32717	**Symptoms:** An interworked call will find its video bandwidth capped at 2mbps in one

Identifier	Summary
	direction. **Conditions**: Video sent from the SIP side to the H323 will be capped at 2mbps. This may result in a different codec being chosen, or a lower bandwidth on the preferred codec. **Workaround**: none.
CSCtx91866	**Symptoms**: If a presence request has expired and VCS receives a 5xx response code in response to the Notify it sends, VCS will not clear the presence subscription. **Conditions**: None. **Workaround**: None.
CSCtw75137	**Symptoms**: Call from an H.323 endpoint with a UTF-16 H323-ID, behind a VCS Control, to a SIP-registered endpoint on a VCS Expressway fails. **Conditions**: For this problem, the H.323 endpoint with a UTF-16 ID must be behind a VCS Control, with a SIP-registered endpoint behind a VCS Expressway. The VCSE is interworking the call and rejects the call attempt. **Workaround**: Use non-UTF-16 H.323 IDs in such a scenario.
CSCtx34718	**Symptoms**: VCS restarts with an Incident report reporting "ACR: TTSSL_closeSession Line: 262". **Conditions**: VCS under heavy load. **Workaround**: None.
CSCtw89950	**Symptoms**: VCS fails to tear down H323 leg on interworked H323 -> SIP call which is transferred (Multiway). **Conditions**: None. **Workaround**: None. **Additional Information**: If VCS requests a SIP call to be cleared (BYE) but never gets an ACK, it should clear the call, including the H.323 leg if a BYE is received on the SIP side.
CSCtw82611	**Symptom**: Presentation is shown as a black screen to all participants in the MCU conference. **Conditions**: C-series codec (C40 and C60 tested so far) running TC4.2.0 calls (SIP) into an MCU conference (4.2(1.43)) (H323 only) with another movi participant running (4.2) (Calls are interworked by the VCS). The C-series codec shares presentation to the conference. Then the C-series uses its multi-site to patch in an audio-only participant (This part does not need to be interworked to recreate the bug). After 15 minutes of all participants being in the conference, if the C-series endpoint stops presentation and starts it again, members of the conference see a black screen instead of the presentation. **Workaround**: None currently known.
CSCtx24759	**Symptoms**: The VCS suffers high CPU load when Presence is in use, leading to reduced responsiveness. **Conditions**: In versions prior to X5.2, the default value for retries in the Presence User Agent was 5 seconds. This was changed to 1800 seconds, but existing configuration was not updated during upgrades. This causes unnecessary retries in situations where some domains on a VCS do not have a presence server. **Workaround**: Set the value to the new default with the following CLI command: xConfiguration Applications Presence User Agent RetryDelta: 1800
CSCtx33677	**Symptom**: An interface on the VCS appears to be unreachable to the network. **Conditions**: VCS X7 or later, with the dual nic key and both interfaces on the same subnet. **Workaround**: Move the interfaces to different subnets. **Resolution**: Explicitly stated in the X7.1 help/admin guide that "The LAN 1 and LAN 2 interfaces must be on different, non-overlapping subnets."
CSCty01037	**Symptoms**: Success of audio-only H.323 calls being invited into a Multiway conference by a SIP endpoint via a VCS may not be correctly reported to the SIP endpoint. This leads to the SIP endpoint (e.g. C40) failing on Multiway Join. **Conditions**: This requires the VCS to be acting as an H.323/SIP interworking gateway, with a neighbored MCU. The H.323 participants are audio-only, and a SIP participant (such as a C40) is the Multiway initiator. On initiating Multiway Join, the feedback of success is not correctly returned to the SIP endpoint.

Identifier	Summary
	Workaround: This problem will not occur on H.323 only.

Resolved in X7.0.3

Identifier	Summary
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.
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.
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.
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

Identifier	Summary
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 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.

Identifier	Summary
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.
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.
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.
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.
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.
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

Identifier	Summary
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.

Resolved in X7.0

Security-related issues

Identifier	Summary
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.
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.

Identifier	Summary
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
CSCtr80205	**Symptoms**: Cisco VCS may include a version of PHP that may be vulnerable to published vulnerabilities. The vulnerabilities are detailed by the following CVE id: CVE-2010-4697, CVE-2006-7243 **Conditions**: None **Workaround**: None **Further Problem Description**: The vulnerability is not confirmed to be exploitable or Cisco VCS, however Cisco is improving VCS product security by upgrading PHP to the latest available version. Additional information about the specific vulnerabilities listed above including condition and possible workarounds can be found by looking at the description of each CVE-id at : http://cve.mitre.org/cve/ . 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 6.8/6.1: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:P/I:P/A:P/E:POC/RL:U/RC:C CVE ID CVE-2010-4697, CVE-2006-7243 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
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: 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

Identifier	Summary
	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

Identifier	Summary
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.
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.
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.
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.
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.
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.

Open caveats

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

Identifier	Summary
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.
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.
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.
CSCtu21769	**Symptoms:** Java vulnerabilities have been observed on Cisco VCS running X7.0.1. **Conditions:** Discovered on a Cisco VCS X7.0.1. **Workaround**: This issue is triggered by the Java application that is run on VCS for legacy TMS Agent provisioning and legacy OCS Relay. Customers using the provisioning feature should migrate to the new TMS Provisioning Extension. Customers using the legacy OCS Relay feature should use the Microsoft OCS/Lync B2BUA. **Additional Information**: In X8 Java will be removed from the VCS product.
CSCtw93381	**Symptoms**: No video on CTS endpoint on CUCM to VCS trunked call after hold/resume. **Conditions**: None. **Workaround**: None. **Additional Information**: See RFC 3711.
CSCty93737	**Symptom**: It is not possible to cluster a set of VCS peers using IPv6 addresses. The following is seen on the clustering page: ' Unknown: aaaa:bbbb:cccc:dddd::eeee:46854 ' And an alarm is raised: 'Invalid cluster configuration. The cluster configuration is invalid - Raised - Warning - Check the Clustering page and ensure that this system's IP address is included and there are no duplicate IP addresses' **Conditions**: VCS running in an IPv6 environment. **Workaround**: No work around.
CSCty82416	**Symptom**: Resource usage page shows “Max (peak)” registrations of 2500 and there is a “Capacity warning: the number of concurrent registrations has approached the licensed limit” alarm. The warning remains present in VCS (acknowledged) and that triggers tickets in TMS. **Workaround**: There is no command option to reset the “Max (peak)” counters and thus remove the alarm. The only way to reset them from VCS is to restart or reboot the VCS.
CSCua72781	**Symptoms**: Remote ringing tone will not be heard on an endpoint registered to VCS Expressway. **Conditions**: Ringing tones sent as "Early Media" via SDP on a provisional response (183 or 180) will not be forwarded. **Workaround**: None. Note this does not affect a call after it has been answered, only the audio ringing tone.
CSCua78996	**Symptoms**: The VCS web interface may become slow or non-responsive, H.323 endpoint/SIP

Identifier	Summary
	UA registrations may fail, etc. due to CPU utilization level. To verify VCS CPU utilization status, access VCS as root user from console or ssh and execute "top" command (Ctrl + C to stop and return to the command line). If your VCS is affected by this reporting issue, you can expect to see high CPU utilization. **Conditions**: A leap second change caused a Linux/Java bug to be exposed, resulting in high CPU utilization. The root of the behavior is located in the Linux kernel when running Java, where a leap second handled by the NTP subsystem results in a livelock situation. On VCS, Java is used for legacy TMS Agent provisioning and legacy OCS Relay. **Workaround**: VCS will recover from high CPU utilization by performing one of the following: ■ Restart VCS (recommended method) ■ Access the VCS as root user via console/ssh and execute, date -s "`date -u`", command **Additional Information**: This issue is triggered by the Java application that is run on VCS for legacy TMS Agent provisioning and legacy OCS Relay. Customers using the provisioning feature should migrate to the new TMS Provisioning Extension to avoid future leap second problems (TMS Provisioning Extension does not use Java). Customers using the legacy OCS Relay feature should upgrade VCS to the X7.1 release or later (code has been updated and will not hit this leap second issue).

Interoperability

The systems below have been tested with this software release.

Gatekeepers / traversal servers

Equipment	Software revision
Cisco VCS	X6.1, X7.0.n, X7.1, X7.2
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)	15.1-4
Cisco TelePresence Advanced Media Gateway	1.1

IP PBXs

Equipment	Software revision
Cisco Unified Communications Manager	8.6.1

Conferencing

Equipment	Software revision
Cisco TelePresence Conductor	XC1.2
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 / Jabber Video	4, 4.1, 4.2, 4.3, 4.4
Microsoft Office Communicator / Lync	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.n TC5.n	
Cisco TelePresence System EX60	TC4.n TC5.n	
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, 4.10.1	See Known limitations section
Polycom HDX 9000	3.0.0.2, 3.0.4	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 3.0.4 / 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 a response to a Cisco VCS interworked SIP INVITE request (because it contains a “Session-Expires” header without a “Supported: timer” extension). Polycom have stated that this will be fixed in a future release.
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 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.

Planned changes for future releases

Future versions of Cisco VCS are expected to remove the following features:

- Telnet access (to improve product security)
- OCS Relay (instead, you are recommended to use the Microsoft OCS/Lync B2BUA to route SIP calls between the VCS and a Microsoft OCS/Lync Server)
- TMS Agent (instead, if you use TMS provisioning, you are recommended to use TMS Provisioning Extension services)

Upgrading to X7.2.n

CAUTION: If you are upgrading a cluster, you must follow the directions in the X7.2 "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 X7.2 "Cluster creation and maintenance" deployment guide (document D14367) contains full instructions on how to upgrade to VCS X7.2 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.

You are recommended to switch to TMS Provisioning Extension (TMSPE) mode, if you are using Cisco TMS with Provisioning or FindMe, when the upgrade to X7.2 is complete and proven to be operating correctly. To switch to Provisioning Extension mode (from TMS Agent legacy mode), you must upgrade TMS to TMS 13.2 or later. Refer to the TMS Provisioning Extension Installation Guide.

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 X7.2 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 X7.2 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.n and replicate your Cisco VCS FindMe accounts with Cisco TMS.

Basic Cisco VCS X7.2 upgrade procedure

Follow this procedure for upgrading Cisco VCS to X7.2, 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 occur if:

   - VCS carries out a disk file system check – which it does approximately once every 30 restarts
   - Provisioning is enabled (in TMS Agent legacy mode), and database re-indexing is in progress – this may take up to 30 minutes if there is a large amount of user data

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.n. You must first upgrade to X5.2 and then to X7.n. See the X5.2 release note, document reference D50582, for details.

Installing language packs

You can install new language packs or install an updated version of an existing language pack.

Language packs are downloaded from the same area on cisco.com from where you obtain your VCS software files. All available languages are contained in one language pack zip file. Download the appropriate language pack version that matches your software release.

After downloading the language pack, unzip the file to extract a set of .tlp files, one per supported language.

To install a .tlp language pack onto the VCS:

1. Go to the **Language** page (**Maintenance > Language**).
2. Click **Browse** and select the .tlp language pack file you want to upload. See the available languages reference table below.
3. Click **Install**.
   The selected language pack is then verified and uploaded
4. Repeat steps 2 and 3 for any other languages you want to install.

To set the default system language:

1. Go to the **Language** page (**Maintenance > Language**).
2. Select the **System default language** from the set of installed languages.
3. Click **Save**.

To use an alternative language from the default language (on a per user and per browser basis):

1. Log in to the VCS using the relevant administrator account.
2. Go to the **Language** page (**Maintenance > Language**).
3. Select the language to use for **This browser** from the set of installed languages.
4. Click **Save**.

Available languages

The following table lists the set of languages currently available and the .tlp filename used to refer to that language.

Language	.tlp filename format
Chinese (Simplified)	vcs-lang-zh-cn_<ver>.tlp
French	vcs-lang-fr-fr_<ver>.tlp
German	vcs-lang-de-de_<ver>.tlp
Japanese	vcs-lang-ja-jp_<ver>.tlp
Korean	vcs-lang-ko-kr_<ver>.tlp
Russian	vcs-lang-ru-ru_<ver>.tlp
Spanish	vcs-lang-es-es_<ver>.tlp

Note that:

- English (en_us) is installed by default and is always available.
- You cannot create your own language packs. Language packs can be obtained only from Cisco.

Using the Bug Search Tool

The Bug Search Tool contains information about open and resolved issues for this release and previous releases, including descriptions of the problems and available workarounds. The identifiers listed in these release notes will take you directly to a description of each issue.

To look for information about a specific problem mentioned in this document:

1. Using a web browser, go to the Bug Search Tool.
2. Sign in with a Cisco.com username and password.
3. Enter the bug identifier in the **Search** field and click **Search**.

To look for information when you do not know the identifier:

To look for information when you do not know the identifier:

1. Type the product name in the **Search** field and click **Search**.
2. From the list of bugs that appears, use the **Filter** drop-down list to filter on either *Keyword*, *Modified Date*, *Severity*, *Status*, or *Technology.*

Use **Advanced Search** on the Bug Search Tool home page to search on a specific software version.

The Bug Search Tool help pages have further information on using the Bug Search Tool.

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 in the documentation, check the web site at http://www.cisco.com/cisco/web/support/index.html where you will be able to:

- Make sure that you are running the most up-to-date software.
- Get help from the Cisco Technical Support team.

Make sure you have the following information ready before raising a case:

- Identifying information for your product, such as model number, firmware version, and software version (where applicable).
- 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 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 (Control with Expressway)	D14651
Cisco VCS Deployment Guide – Cisco VCS Starter Pack Express	D14618
Cisco VCS Deployment Guide – FindMe	D14525
Cisco VCS Deployment Guide – Cisco Unified Communications Manager with Cisco VCS	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 – External policy on Cisco VCS	D14854
Cisco VCS Deployment Guide – Device authentication on Cisco VCS	D14819
Cisco VCS Deployment Guide – Virtual Machine	D14951
Cisco TelePresence Multiway Deployment Guide	D14366
Cisco TMS Release Note	D14741
Cisco TMS Installation Guide	D14389
Cisco TMS Administration Guide	D13741
Cisco TMS Provisioning Deployment Guide	D14368
TMS Provisioning Extension Deployment Guide	D14941

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

Secure communications

For secure communications (HTTPS and SIP/TLS) we recommend that you replace the VCS default certificate with a certificate generated by a trusted certificate authority. See *Certificate Creation and Use with VCS Deployment Guide* for more information about to how to generate certificate signing requests and install certificates.

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.

RFCs

The following RFCs are supported within the VCS X7 release:

RFC	Description
791	Internet Protocol
1213	Management Information Base for Network Management of TCP/IP-based internets
1305	Network Time Protocol (Version 3) Specification, Implementation and Analysis
2327	SDP: Session Description Protocol
2460	Internet Protocol, Version 6 (IPv6) Specification (partial, static global addresses only)
2464	Transmission of IPv6 Packets over Ethernet Networks
2782	A DNS RR for specifying the location of services (DNS SRV)
2915	The Naming Authority Pointer (NAPTR) DNS Resource Record
2976	SIP INFO method
3164	The BSD syslog Protocol
3261	Session Initiation Protocol
3263	Locating SIP Servers
3264	An Offer/Answer Model with the Session Description Protocol (SDP)
3325	Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
3326	The Reason Header Field for the Session initiation Protocol (SIP)
3265	Session Initiation Protocol (SIP) – Specific Event Notification
3327	Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts
3489	STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
3515	The Session Initiation Protocol (SIP) Refer Method
3550	RTP: A Transport Protocol for Real-Time Applications
3581	An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing
3596	DNS Extensions to Support IP Version 6
3761	The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)
3856	A Presence Event Package for the Session Initiation Protocol (SIP)
3863	Presence Information Data Format (PIDF)
3880	Call Processing Language (CPL): A Language for User Control of Internet Telephony Services
3891	Replaces header
3892	Referred-by header
3903	Session Initiation Protocol (SIP) Extension for Event State Publication
3944	H.350 Directory Services
3986	Uniform Resource Identifier (URI): Generic Syntax
4028	Session Timers in the Session Initiation Protocol
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers
4291	IP Version 6 Addressing Architecture

RFC	Description
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
4479	A Data Model for Presence
4480	RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF)
4787	Network Address Translation (NAT) Behavioral Requirements for Unicast UDP
4861	Neighbor Discovery for IP version 6 (IPv6)
5095	Deprecation of Type 0 Routing Headers in IPv6
5104	Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF): Temporary Maximum Media Stream Bit Rate Request (TMMBR)
5245	Interactive Connectivity Establishment (ICE)
5389	Session Traversal Utilities for NAT (STUN)
5424	The Syslog Protocol
5626	Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)
5627	Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP). Note that this RFC is only partially supported: Public GRUU is supported; Temporary GRUU is not supported.
5766	Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)
5806	Diversion Indication in SIP
6156	Traversal Using Relays around NAT (TURN) Extension for IPv6

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.

Virtual machine

From X7.1 the VCS software can run on VMware.

Before you can order your release key and any option keys, you must first download and install the .ova file in order to obtain your hardware serial number. The VCS provides limited functionality until a valid release key is entered.

Note that the .ova file is only required for the initial install of the VCS software on VMware. Subsequent upgrades should use the .tar.gz file.

See *Cisco VCS Virtual Machine Deployment Guide* for full installation instructions.

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, 6514 TCP	Cisco VCS → Host
LDAP communication	389 TCP	Cisco VCS → Host
LDAPS communication	636 TCP	Cisco VCS → Host
TMS Provisioning Extension services	443 TCP	Cisco VCS → Cisco TMS
IPSEC cluster communication	500 UDP	Cisco VCS ↔ Cisco VCS
Intra-cluster communication	IP Protocol 51 (IPSec AH)	Cisco VCS ↔ Cisco VCS
Device provisioning (TMS Agent)	389 TCP	Cisco TMS → Cisco VCS
Device provisioning replication (TMS Agent)	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
Media (Assent, H.460.19 multiplexed media)*	2776:2777 UDP	Host → Cisco VCS
Media (H.460.19 non-multiplexed media)*	50000:54999 UDP	↔
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
SIP media (RTP, RTCP) (non-traversal)*	50000:54999 UDP	↔
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.

Third-party software

Third-party software used in the Cisco VCS includes:

Package name	Version
Apache	2.4.2
OpenSSL	1.0.1c

This product includes copyrighted software licensed from others. A list of the licenses and notices for open source software used in this product can be found at: http://www.cisco.com/en/US/products/ps11337/products_licensing_information_listing.html.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.