Cisco TelePresence Video Communication Server X8.2.2

Software Release Notes
October 2014

Contents

Product documentation

The following documents provide guidance on installation, initial configuration, and operation of the product:

- Cisco VCS Administrator Guide
- Cisco VCS Getting Started Guide
- Cisco VCS Cluster Creation and Maintenance Deployment Guide
- Cisco VCS on Virtual Machine Installation Guide
- Cisco TMS Provisioning Extension Deployment Guide

Further VCS deployment guides covering basic configuration, Cisco VCS Starter Pack Express, FindMe, device authentication, certificate creation and use, ENUM dialing, external policy, integration with Cisco Unified Communications Manager, Microsoft Lync, and Cisco Unity Connection are available on cisco.com.

Changes in X8.2.2

VCS version X8.2.2 is a maintenance release and does not introduce any new features or major changes to behavior. See Resolved issues [p.9] and Open issues [p.17] for changes since the previous release.

Changes in X8.2.1

VCS version X8.2.1 is a maintenance release and does not introduce any new features or major changes to behavior. See Resolved issues [p.9] and Open issues [p.17] for changes since the previous feature release.

New features in X8.2

Unified Communications: Jabber Guest

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

External XMPP federation

External XMPP federation enables users registered to Unified CM IM & Presence to communicate via the VCS Expressway with users from a different XMPP deployment.

TURN media over TCP

The VCS Expressway TURN server supports TURN media over TCP.

This allows clients to use TURN services in environments where UDP connections are not supported or blocked. Configuration of the supported protocols is available only through the CLI command **`xConfiguration Traversal Server TURN ProtocolMode`**.

New 'Unified Communications traversal' zone type

To simplify the configuration of secure traversal client and traversal server zones that are to be used for Unified Communications, you must now use the new zone type of *Unified Communications traversal* when configuring zones via the web interface.

This automatically configures an appropriate traversal zone (a traversal client zone when selected on a VCS Control, or a traversal server zone when selected on a VCS Expressway) that uses SIP TLS with **TLS verify mode** set to *On*, and **Media encryption mode** set to *Force encrypted*.

This replaces the previous **Unified Communications services** setting that was available when configuring traversal client and traversal server zones. Existing zones configured in previous software versions for **Unified Communications services** are automatically converted to use the new *Unified Communications traversal* zone type.

Note that this zone type applies to the web interface only, the underlying CLI configuration settings have not changed.

Support for `X-cisco-srtp-fallback`

Support has been added for the **`X-cisco-srtp-fallback`** package, allowing the VCS's B2BUA to use Cisco Unified Communications Manager-style best effort media encryption for the automatically generated TLS neighbor zones.

RTP and RTCP media demultiplexing ports

In Small/Medium systems, 1 pair of RTP and RTCP media demultiplexing ports are used. These can now either be explicitly specified (**Configuration > Traversal > Ports**) or they can be allocated from the start of the general range of traversal media ports. In previous X8 releases they were always allocated from the start of the traversal media ports range.

In Large systems, 6 pairs of RTP and RTCP media demultiplexing ports are used. These are still always allocated from the start of the traversal media ports range.

After upgrading to X8.2, all existing traversal media port configurations / firewall requirements are maintained.

Diagnostic logging

The diagnostic logging feature has been extended to include:

- an xconfig file
- an xstatus file
- enabling the tcpdump (if requested) cluster-wide
- consolidating all of the files into a single downloadable diagnostic log archive (per peer)
- an indication on the web administration page of which user / IP address initiated the logging

The xconfig and xstatus files are taken at the start of the logging process.

SIP REFER support

The VCS B2BUA has SIP REFER message support. A **SIP REFER mode** advanced zone configuration parameter has been introduced.

By default it will forward REFER messages, but it can be configured to terminate REFER messages and use the B2BUA to perform the transfer (typically to a bridge) on behalf of the far endpoint.

Other enhancements and usability improvements

- The **HTTP server allow list** page (used for mobile and remote access clients to access additional web services inside the enterprise) now displays any automatically configured entries.
- You can configure the timeout period for TLS socket handshake (**Configuration > Protocols > SIP**).
- The TURN relay status page (**Status > TURN relay usage**) now provides a summary list of all the clients that are connected to the TURN server. From there you can select a specific client to see all of the relays and ports that it is using.
- Ability to copy search rules. You can use the **Clone** action on the search rules listing page (**Configuration > Dial plan > Search rules**) to copy and then edit an existing search rule.
- The DNS lookup tool allows you to select which DNS servers (from the configured set of default DNS servers) to use for the lookup.
- The automated protection service now supports IPv6 addresses.

Changed functionality

Access to the systemunit.xml file is now protected. Only authenticated VCS administrator accounts can access the file. This may affect the discovery of VCS by Cisco TMS.

Call status and call history now indicates components routed through the B2BUA for encryption or ICE support with a component type of 'B2BUA' (formerly 'Encryption B2BUA').

Note: The combination of having static NAT mode on and having the B2BUA engaged to do media encryption/decryption can cause the firewall outside the VCS Expressway to mistrust packets originating from the VCS Expressway. You can work around this by configuring the firewall to allow NAT reflection. If your firewall cannot allow this, you must configure the traversal path such that the B2BUA on the VCS Expressway is not engaged.

Changes in X8.1.1

Unified Communications: mobile and remote access

Cisco Unified Communications mobile and remote access is a core part of the Cisco Collaboration Edge Architecture. It allows endpoints such as Cisco Jabber to have their registration, call control, provisioning, messaging and presence services provided by Cisco Unified Communications Manager (Unified CM) when the endpoint is not within the enterprise network. The VCS provides secure firewall traversal and line-side support for Unified CM registrations.

For more information including configuration recommendations and troubleshooting details, see *Unified Communications: Mobile and Remote Access via VCS Deployment Guide*.

Support to modify Maximum transmission unit (MTU) size

You can configure the maximum transmission unit (MTU) for each network interface on the **System > IP** page.

Diagnostic logging

The tcpdump facility has been removed from the **Diagnostic logging** tool.

Jabber Guest

Jabber Guest support has been removed (it was previously provided as a feature preview in X8.1). It will be reintroduced in a future release of VCS software.

New features in X8.1

Microsoft Lync 2013 / H.264 SVC support

The Microsoft Lync B2BUA now supports calls to and from Microsoft Lync 2013 clients. It provides interworking between standard H.264 AVC and Lync 2013's H.264UC SVC codec. To use Lync 2013 you must install the **Microsoft Interoperability** option key (formerly known as the **Enhanced OCS Collaboration** option key). Note that for Lync 2010, the **Microsoft Interoperability** option key requirements remain as per previous releases (i.e. it is required for encrypted calls to and from Microsoft Lync Server and for establishing ICE calls to Lync clients).

Presentation sharing via Lync 2013 is supported but only from VCS to Lync.

Support for standards-based H.264 SVC codecs

The B2BUA now supports calls to standards-based H.264 SVC codecs.

Improved performance and scalability

- VCS X8.1 software can take advantage of the improved performance and scalability capabilities that are available when running on Large VM server deployments. It can support up to 500 traversal calls, 750 non-traversal calls and 5000 registrations. Note that standard VCS appliances or equivalent VM hardware still

provides support for up to 150 traversal calls, 750 non-traversal calls and 2500 registrations.

- The number of concurrent searches has increased from 100 to 500.

New traversal media port framework

- For new installations of X8.1 or later, the default range for **traversal media ports** is 36000 – 59999. The previous default range of 50000 - 54999 still applies to earlier releases that have upgraded to X8.1. The larger range is required to support the improved scalability features.
- The media demultiplexing ports on the VCS Expressway now use the first set of ports from the general range of **traversal media ports** instead of 2776 and 2777.
  - On existing systems that have been upgraded to X8.1, this will be 50000 and 50001 by default.
  - On new installations of X8.1, this will be 36000 and 36001 by default.
  - On large VM deployments, the first 12 ports in the traversal media port range are used (50000 - 50011 or 36000 - 36011 as appropriate).

  This applies to all RTP/RTCP media, regardless of whether it is H.323 or SIP. Thus, the previously used **Media demultiplexing RTP port** and **RTCP port** settings (**Configuration > Traversal > Ports**) and associated **`xConfiguration Traversal Server`** CLI commands have been removed. Administrators will need to adjust their firewall settings accordingly.

New TURN server port framework

On Large systems you can configure a range of TURN request listening ports. The default range is 3478 – 3483.

For new installations of X8.1 or later, the default range for **TURN relay media ports** is 24000 – 29999. The previous default range of 60000 – 61799 still applies to earlier releases that have upgraded to X8.1.

Delegated credential checking for device authentication (SIP only)

By default, the VCS uses the relevant credential checking mechanisms (local database, Active Directory Service or H.350 directory via LDAP) on the VCS performing the authentication challenge.

Alternatively you can now configure the VCS so that the credential checking of SIP messages is delegated, via a traversal zone, to another VCS. Delegated credential checking is useful in deployments where you want to allow devices to register on a VCS Expressway, but for security you want all communications with authentication systems (such as an Active Directory server) to be performed inside the enterprise.

Credential checking for both Digest and NTLM messages may be delegated.

Automated protection

An automated intrusion protection feature has been added. It can be used to detect and block malicious traffic and to help protect the VCS from dictionary-based attempts to breach login security.

It works by parsing the system's log files to look for repeated failures to access specific service categories, such as SIP, SSH and web/HTTPS access. When the number of failures within a specified time window reaches the configured threshold, the source host address (the intruder) is blocked for a period of time. You can configure sets of addresses that are exempted always from one or more categories.

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

Licensing of audio-only SIP traversal calls

Audio-only SIP traversal calls are now treated distinctly from video SIP traversal calls. Each traversal call license allows either 1 video call or 2 audio-only SIP calls. Hence, a 100 traversal call license would allow, for example, 90 video and 20 SIP audio-only simultaneous calls. Any other audio-only call (non-traversal, H.323 or interworked) will consume a standard video call license (traversal or non-traversal as appropriate).

The **Overview** and **Resource usage** pages show separate counts for video and audio-only SIP traversal calls.

Note that:

- VCS defines an "audio-only" SIP call as one that was negotiated with a single “m=” line in the SDP. Thus, for example, if a person makes a “telephone” call but the SIP UA includes an additional m= line in the SDP, the call will consume a video call license.
- While an "audio-only" SIP call is being established, it is treated (licensed) as a video call. It only becomes licensed as "audio-only" when the call setup has completed. This means that if your system approaches its maximum licensed limit, you may be unable to connect some "audio-only" calls if they are made simultaneously.

TMS Agent functionality removed

TMS Agent (legacy mode) functionality has been removed. Instead, if you use TMS provisioning, you must use TMS Provisioning Extension services.

Java application removed

The Java application has been removed. This removes the threat of Java security vulnerabilities.

OCS Relay functionality and Microsoft OCS 2007 zone profile removed

OCS Relay functionality and the Microsoft Office Communications Server 2007 zone profile have been removed. The Cisco AM GW configuration options previously under the VCS configuration menu, and the Cisco Advanced Media Gateway zone profile have also been removed.

Instead, we recommend that you use the Microsoft Lync B2BUA to route SIP calls between the VCS and a Microsoft Lync Server, and to configure your Cisco AM GWs as B2BUA transcoders. Note that B2BUA connections to Microsoft OCS are no longer supported from X8.1.

Support for Active Control

VCS supports Active Control (iX Channel passthrough) as supported by Cisco TelePresence Server 3.1 or later and endpoints running TC6.2 or later. It can be configured on a per-zone basis.

FIPS140-2 cryptographic mode

VCS has implemented FIPS140-2 compliant features.

New VMware installations

New VMware installations have a choice of 3 .ova files: **Small** (for Cisco Business Edition 6000 deployments), **Medium** (for typical deployments) or **Large** (for large-scale deployments). Note that the VM .ova files are used for new installations only. Do not use them to upgrade your existing VM installation.

See *VCS on Virtual Machine Installation Guide* for information about deploying on UCS tested reference configurations and their associated memory and CPU resource reservation requirements.

ICE messaging support

ICE messaging support is now configurable at the zone and subzone level.

Certificate management

The certificate management pages are now located under **Maintenance > Security certificates**:

- The management of CA certificates has been improved, allowing you to view, upload and delete individual CA certificates.
- The VCS's server and trusted CA certificates can be viewed in either a human-readable, decoded format, or in their raw, PEM format.

Other enhancements and usability improvements

- The online help has a new skin and an improved search capability.
- There is a new *Cisco Unified Communications Manager (8.6.1 or later)* zone profile. This profile supports BFCP and should be used in SIP trunk neighbor zones to Unified CM running version 8.6.1 or later.
- The ephemeral port range can be configured via the web interface (**System > Administration**).
- Maintenance mode can be configured via the web interface (**Maintenance > Maintenance mode**).
- The Microsoft Lync B2BUA supports multiple TURN servers.
- The **Lync B2BUA status** page now shows the number of active calls, and resource usage as a percentage of the number of allowed Lync B2BUA calls.
- A B2BUA service restart is no longer required to enable changes to the list of trusted hosts to take effect.
- A contact email address and a proxy server can be specified when configuring the incident reporting server.
- The DNS cache is flushed automatically whenever any DNS configuration is changed (**System > DNS**). The **DNS** page also contains a manual option to flush the DNS cache.
- When logging in, you now have to choose the administrator login option only if you are using "standalone FindMe" i.e. FindMe without Cisco TMSPE.
- CPL location node supports regex-based source alias rewriting.
- Active Directory Service configuration: you can specify an override value for the NetBIOS machine name if the **System host name**, which is used as the default name, exceeds 15 characters.
- Previously-installed language packs can be deleted.
- The VCS Starter Pack Express supports device provisioning for SX20 endpoints. Note: this is a preview feature.
- You have the option to take a tcpdump while diagnostic logging is in progress.
- SIP network logging at the DEBUG level now includes the local address and port (as well as the destination/source information).
- You can specify the transport type to use for SIP calls from a DNS zone, when DNS NAPTR records and SIP URI parameters do not provide the preferred transport information.
- The VCS supports time-limited option keys. The options keys page displays the validity period of each key. All pre-existing option keys have an *Unlimited* validity period.
- Filtering options are only displayed on status and list pages if there is more than one page of information to display. Status and list pages show 200 records per page, except for Log pages which show 1000 records per page.
- When configuring firewall rules:
  - You can choose whether to drop or reject denied traffic. On upgrade to X8.1 or later, any existing "deny" rules will now drop the traffic; prior to X8.1 the traffic would have been rejected.
  - If you have made several changes there is now an option to revert all changes. This discards all pending changes and resets the working copy of the rules to match the current active rules.

  - You can more easily change the order of the rules by using up/down arrow buttons to swap the priorities of adjacent rules.
  - Rules can be configured for XMPP traffic.
- The **Search rules** page now indicates if the target zone of a rule is unavailable.
- Port conflict alarms now indicate the exact features and ports that are in conflict.
- When performing a system backup, the backup filename is now prefixed by the software version number.
- The application now uses CiscoSSL (instead of OpenSSL).
- The xConfiguration and xCommand CLI command sets removed in version X7.2 have been reinstated.
- When using CPL to modify the source URL of a From header, any corresponding display name is also modified to match the username part of the modified source URL.
- Improved web interface usability when switching between SRV and address record resolution modes when configuring the address of an LDAP server for remote user account authentication.

Changed functionality

- For new installations of X8.1 or later, the default range for **ephemeral ports** is 30000 – 35999. Prior to X8.1, the default range was 40000 – 49999. Existing systems upgraded to X8.1 or later will preserve their previous port ranges.
- The **Dual Network Interfaces** option key is now called **Advanced Networking**. When the key is installed you can now configure the use of dual network interfaces separately from the use of static NAT.
- Most system configuration items are now peer-specific (they are not replicated across peers when the VCS is part of a cluster). See "Specifying peer-specific items in clustered systems" in *VCS Administration Guide* for more information.
- New installations of VCS software now ship with a temporary trusted CA, and a server certificate issued by that temporary CA. We strongly recommend that you replace the server certificate with one generated by a trusted certificate authority, and that you install CA certificates for the authorities that you trust. If you upgrade to this release from an earlier installation of VCS software, your existing server and trusted CA certificates will not be affected.
- When configuring the sources for administrator account authentication, the *Remote* option is now labeled as *Remote only*.
  This also means you can no longer access the VCS via the default **admin** account if a *Remote only* authentication source is in use. The *Local* option has also been renamed to *Local only*. Note: do not use *Remote only* if VCS is managed by Cisco TMS.
- The **Reboot**, **Restart** and **Shutdown** maintenance options have been combined into one **Restart options** page.
- When starting a diagnostic log, the relevant system modules now have their log levels automatically set to "debug" and are automatically reset to their original values when logging is stopped.
- You can no longer access the system over Telnet.
- The **Expressway** option key is now called **Traversal Server**.
- The DNS **Local host name** is now referred to as the **System host name**.
- *Auditor* access level now includes the **Alarms** page.
- The login account configuration pages are now accessed under a new top-level **Users** menu (previously under **Maintenance > Login accounts**).
- The **Clustering** page is now accessed under the **System** menu.
- The **System administration** page is now accessed under **System > Administration**.
- The **Firewall rules configuration** pages are now accessed under **System > Protection**.

- The **VCS configuration** menu is now called just **Configuration**.
- The **SIP** page is now accessed directly via **Configuration > Protocols > SIP** and the **Domains** page is now accessed via **Configuration > Domains**.
- The **Calls** page and menu is now called **Call routing**. **Call routed mode** is now called **Call signaling optimization** and the options are *On* and *Off*.
- On the VCS Expressway, the **VCS configuration > Expressway** menu is now **Configuration > Traversal**.
- All references to **OCS/Lync B2BUA** have been renamed to refer to **Lync B2BUA**. The **Enhanced OCS Collaboration** option key is now called **Microsoft Interoperability**.
- References to 'Movi' have been changed to 'Jabber Video'.
- The **FindMe configuration** page is now accessed directly under **Applications > FindMe**.
- On the **Upgrade** page, the **VCS platform** component is now referred to as **System platform**.
- The **Advanced account security** page is now called **Advanced security** and is accessed via **Maintenance > Advanced security**.
- The **Local VCS inbound ports** page is now called **Local inbound ports**, and the **Local VCS outbound ports** page is now called **Local outbound ports**.
- The advanced zone configuration **Empty INVITE allowed** setting is now referred to as **Send empty INVITE for interworked calls**.
- The following settings have been removed from the **SIP configuration** page: **Require UDP BFCP mode** and **Require Duo Video mode**. They existed to provide support for interoperability issues with old versions of Cisco TelePresence MXP endpoints. These settings can still be configured via the CLI if necessary.
- The **Login account authentication configuration** page has been removed, and the **Administrator authentication source** and **FindMe authentication source** settings are now on the **Login account LDAP configuration** page.
- The `xConfiguration Interworking Require Invite Header Mode` is now `Off` by default.
- The **Directory** option has been removed from the list of restriction policies on the **Registration configuration** page and the list of Call Policy modes on the **Call Policy configuration** page.
- The DNS lookup tool includes Unified Communications SRV services.

Resolved issues

Resolved in X8.2.2

To find the latest information about defects in this release, use the Cisco Bug Search Tool.

Resolved in X8.2.1

Table 1: Issues resolved in X8.2.1

Identifier	Description
CSCup29435	**Symptoms:** VCS reports an application error, and the process restarts automatically. An alarm is raised reporting that an unexpected software error was detected. **Conditions:** Rare, under investigation. **Workaround:** None, the app process will automatically be restarted.

Table 1: Issues resolved in X8.2.1 (continued)

Identifier	Description
CSCup46518	**Symptoms:** A remote endpoint registered to UCM via Mobile and Remote Access may fail to register if a VCS Control in the cluster is out of service (shutdown, or otherwise unreachable). **Conditions:** One VCS Control in the cluster is out of service, and the route created by the endpoint happens to use that server. **Workaround:** Restart the endpoint, which will cause it to obtain updated information about the available VCS Control servers, which will not include the one that is out of service.
CSCup01126	**Symptoms:**VCS restart due to internal application crash with "An unexpected software error was detected in app[15225]: SIGSEGV (address not mapped to object) @0x0000000000000000" alarm message.
CSCup29484	**Symptoms:** For re-INVITE process, VCS B2BUA reuse Max-Forwards value that it stored at the call establishment, therefore may see Max-Forward parameter reduced to an unexpected level. **Conditions:** Re-INVITE and call go through VCS B2BUA application. **Workaround:** None.
CSCup93352	**Symptoms:** Phonebook lookups fail for Cisco Jabber Video for TelePresence users. Diagnostic logs show: Module="developer.phonebook" Level="ERROR" CodeLocation="phonebook_logging(21)" Detail="Failed to handle INFO request" Exception="UserNotFound('dial_ string=deviceurii@domain',)" Message="INFO sip:phonebook@domain SIP/2.0 **Conditions:** This Cisco Jabber Video for TelePresence account has been signed into from more than one computer. At present this is believed to only affect VCS version X8.2. **Workaround:** Remove provisioning status UUID which have duplicate "dial_string" parameter. 1) Run query to check latest provisioning device status on VCS Control where provisioning service is running 2) Search UUID of user reporting phonebook service issue (or duplicate dial string entries) 3) Run RestAPI to "Delete" those duplicate entries 4)User must re-login after you DELETE the provisioning status
CSCup75947	**Symptoms:** On VCS running 8.2 in a CMR Hybrid environment, B2BUA fails to process and forward on the ACK sent by an MCU in response to a WebEx 200OK. The results in a SIP negotiation failure where the connection ultimately times out on the WebEx side and WebEx sends a BYE. **Conditions:** CMR Hybrid where MCU dials out to WebEx. **Workaround:** In CMR Hybrid deployments you should: ■ Continue to use X7.2.3 software, or ■ Reconfigure the VCS Expressway to not use static NAT, or ■ Recommended configuration for VCS Control with VCS Expressway deployments is to configure the media encryption policy setting on the traversal client zone on VCS Control, the traversal server zone on VCS Expressway, and every zone and subzone on VCS Expressway, and to only use static NAT on the VCS Expressway. With this configuration the encryption B2BUA will only be enabled on the VCS Control.

Table 1: Issues resolved in X8.2.1 (continued)

Identifier	Description
CSCup25151	**Symptom:** The following Cisco products: Cisco TelePresence Video Communication Server include a version of openssl that is affected by the vulnerabilities identified by the Common Vulnerability and Exposures (CVE) IDs: CVE-2010-5298 - SSL_MODE_RELEASE_BUFFERS session injection or denial of service CVE-2014-0076 - Fix for the attack described in the paper "Recovering OpenSSL ECDSA Nonces Using the FLUSH+RELOAD Cache Side-channel Attack" CVE-2014-0195 - DTLS invalid fragment vulnerability CVE-2014-0198 - SSL_MODE_RELEASE_BUFFERS NULL pointer dereference CVE-2014-0221 - DTLS recursion flaw CVE-2014-0224 - SSL/TLS MITM vulnerability CVE-2014-3470 - Anonymous ECDH denial of service This bug has been opened to address the potential impact on this product. **Conditions:** Devices running an affected version of software. **Workaround:** None. **Further Problem Description:** Fix will be available with X8.2.1. **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 10/9.5: https://intellishield.cisco.com/security/alertmanager/cvss?target=new&version=2.0&vector=AV:N/AC:L/Au:N/C:C/I:C/A:C/E:F/RL:U/RC:C The Cisco PSIRT has assigned this score based on information obtained from multiple sources. This includes the CVSS score assigned by the third-party vendor when available. The CVSS score assigned may not reflect the actual impact on the Cisco Product.
CSCup50593	**Symptoms:** VCS reports an application error, an alarm is raised reporting that an unexpected software error was detected (getCallSerialNumbers Line: 41). **Conditions:** The VCS application builds SIP message strings from null pointer. **Workaround:** None.

Resolved in X8.2

Table 2: Issues resolved in X8.2

Identifier	Description
CSCum90139	**Symptoms**: VCS X8.1 uses the Ethernet 2 IP address for the media part in SDP rather than the configured Static NAT IP address. This results in calls failing on the media part. **Conditions**: Running VCS X8.1 with Static NAT and encryption B2BUA enabled (a media encryption policy other than Auto). **Workaround**: Recommended configuration for VCS Control with VCS Expressway deployments is to configure the same media encryption policy setting on the traversal client zone on VCS Control, the traversal server zone on VCS Expressway, and every zone and subzone on VCS Expressway, and to only use static NAT on the VCS Expressway. With this configuration the encryption B2BUA will only be enabled on the VCS Control.

Resolved in X8.1.1

Table 3: Issues resolved in X8.1.1

Identifier	Description
CSCuo16472	**Symptom**: VCS includes a version of OpenSSL that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) ID CVE-2014-0160. This bug has been opened to address the potential impact on this product. **Conditions**: Device with default configuration, running one of the following versions: X7.2 X7.2.1 X7.2.2 X7.2.3 RC2 X8.1. Version X7.1 and all prior versions are NOT vulnerable to this issue. **Workaround**: Not currently available. **Further Problem Description**: Additional details about this vulnerability can be found at http://cve.mitre.org/cve/cve.html **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 5/4.4: https://intellishield.cisco.com/security/alertmanager/cvss?target=new&version=2.0&vector =AV:N/AC:L/Au:N/C:P/I:N/A:N/E:H/RL:OF/RC:C The Cisco PSIRT has assigned this score based on information obtained from multiple sources. This includes the CVSS score assigned by the third-party vendor when available. The CVSS score assigned may not reflect the actual impact on the Cisco Product. CVE-2014-0160 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/web/about/security/psirt/security_vulnerability_policy.html
CSCul12855	**Symptom**: VCS systems enable a number of SSL ciphers by default. The default configuration in X8.1 is: ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:RC4-SHA:HIGH:!ADH:!aNULL. This means that suites that may be affected by issues such as the RC4 weakness (CVE-2013-2566), BEAST (CVE-2011-3389), or Lucky 13 (CVE-2013-0169). By default no GUI method is provided to allow the customization of these values to a customer's security policy. **Conditions**: VCS systems running a version of VCS software prior to X8.1.1. **Workaround**: Customers may modify the ssl.conf file of the device and modify the cipher list to that required to meet their security policy. Customers are advised to consult with Cisco TAC or their authorized support provider for assistance with this modification. **Further Problem Description**: This defect is opened as an enhancement to the current operation of the VCS. Future versions of the product will be modified to remove all known affected ciphers. This may also include a migration to TSL 1.2, and the ability to modify the ciphers in use from the GUI. **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 2.6/2.1: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1 &version=2&vector=AV:N/AC:H/Au:N/C:N/I:P/A:N/E:U/RL:W/RC:C CVE-2013-2566, CVE-2011-3389 and CVE-2013-0169 have 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
CSCul83652	**Symptoms**: All endpoint registrations are lost. A kernel panic is logged in the kernel log. The system continues to run, but network traffic is affected for the VCS application. The only way to recover is to reboot the system. **Conditions**: Occurs only on VCS X8.1. On systems where it does occur, it happens very infrequently. Has only been seen on systems behind a GRE tunnel. **Workaround**: Use a cluster for registration resiliency.

Table 3: Issues resolved in X8.1.1 (continued)

Identifier	Description
CSCul93670	**Symptom**: Unified Communications services fail to start after a VCS restart. Mobile and remote systems will not be able to register to Unified CM or make calls. This is an occasional issue. **Conditions**: Restart (or reboot) a VCS that has Mobile and remote access enabled. **Workaround**: After a restart or reboot, wait 5 minutes and then go to **Status > Unified Communications** in the web interface. If any of the services are in an error state, go to **Configuration > Unified Communications > Configuration** and disable and then re-enable the **Mobile and remote access feature**.
CSCum48012	**Symptom**: Memory leak in the application which causes swap to be used. **Conditions**: Running VCS X8.1. **Workaround**: Monitor memory usage and when usage of swap becomes high, reboot the VCS.
CSCun42369	**Symptom**: In certain scenarios, if you telnet or HTTP on port 443 to a VCS running X7.n or earlier, you will get a bad request error with a hint URL that includes the private IP of the VCS Expressway. Because of the nature of the request, this will not be fixed-up by firewalls. **Conditions**: This is an apache related response issue. **Workaround**: None for X7.n and below. Issue is resolved in X8.1.1 and above which runs a newer version of Apache where no hint URL is provided.

Resolved in X8.1

Table 4: Issues resolved in X8.1

Identifier	Description
CSCue55256	**Symptoms**: Cannot uninstall a language pack. **Conditions**: Install any language pack on VCS. **Workaround**: None. **Additional Information**: From X8.1 you can remove previously-installed language packs via the web interface.
CSCud59255	**Symptoms**: When an H323 call is routed via a cluster configured for Optimal routed mode, the cluster will be removed from the signaling path altogether. **Conditions**: Cluster configured for Optimal routed mode. **Workaround**: Set cluster routed mode to Always. **Additional Information**: This bug can cause calls routed via the cluster showing as duplicate in TMS CDRs/TMS AE with non-identical global call IDs.
CSCtr77670	**Symptom**: 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. **Conditions**: This scenario is more likely to occur in new installations of X7 software which has SIP UDP disabled by default. **Workaround**: Enable SIP UDP.

Table 4: Issues resolved in X8.1 (continued)

Identifier	Description
CSCtu21769	**Symptoms**: Java vulnerabilities have been observed on VCS running X7.0.1. **Conditions**: Discovered on a 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 Cisco TMSPE. Customers using the legacy OCS Relay feature should use the Microsoft Lync B2BUA.
CSCtw93381	**Symptoms**: No video on CTS endpoint on Unified CM 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. **Conditions**: VCS running in an IPv6 environment. **Workaround**: None.
CSCua81035	**Symptoms**: Incident report generated and "application failed" alarm raised with the following message: "An unexpected error was detected in phonebookserver.py: this should never happen" The impact of this bug is that it may cause the phonebook server (or provisioning server) to crash. **Conditions**: The ACR is due to a bug in twisted sip module. It raises a runtime error if a message transmission is aborted while receiving a message. **Workaround**: The phonebook server is automatically restarted in a matter of seconds so there is a limited impact.
CSCua78996	**Symptoms**: The VCS web interface may become slow or non-responsive, H.323 endpoint/SIP UA registrations may fail, etc. due to CPU utilization level. 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. **Workaround**: Restart VCS. **Additional Information**: This issue is triggered by the Java application that is run on VCS for legacy TMS Agent provisioning and legacy OCS Relay.
CSCuc53768	**Symptoms**: Some third-party endpoint registration status shows “unknown and Unknown” for Device Type. **Conditions**: Endpoint does not include valid information for t35CountryCode or/and manufacturerCode in Registration Request. **Workaround**: None.
CSCuc68264	**Symptoms**: Calls fail with 400 (P-Asserted Identity) Unknown SIP URL Prefix **Conditions**: This occurs when PAI includes two URL fields at which seem to be ok according to standard. **Workaround**: None

Table 4: Issues resolved in X8.1 (continued)

Identifier	Description
CSCuc98144	**Symptom**: One way audio. **Conditions**: VCS starts open a logical channel while Master/Slave Determination still going on. **Workaround**: Turn allow empty INVITE off on the zone profile for the CUCM zone. This forces the VCS to send out an initial INVITE with a preconfigured SDP. This allows the call to connect with audio in both directions.
CSCue35446	**Symptoms**: No presentation is seen on the receiving endpoint in a SIP<>H323 interworked call . **Conditions**: In interworked calls (H323<>SIP) involving a VCS Expressway, where the SIP side of the call is on the traversal server side, no presentation is seen on the receiving endpoint if a SIP INVITE has been sent down a traversal server zone without resulting in a call being set up. **Workaround**: Prevent the call scenario interworking between SIP and H323, or prevent the call setup (INVITE) from being sent multiple locations at once.
CSCud41052	**Symptoms**: NTLM authentication fails when NTLMv2 response > 256 bytes long. **Conditions**: If the NtChallengeResponse field in the NTLM authenticate message exceeds 256 bytes in length then NTLM authentication will always fail. **Workaround**: Keep NtChallengeResponse field in the NTLM authenticate message less than 255 bytes long.
CSCud90957	**Symptoms**: An alarm will be displayed saying "An unexpected software error was detected in app: SIGSEGV", and the details will refer to "TerminationPointAddH460ShimLayer.cpp" **Conditions**: This will occur if the Media Forwarding component on a VCS Control, sending towards an VCS Expressway, is using H460 firewall traversal and it receives and tries to forward an empty UDP packet. **Workaround**: None, but the application will automatically restart on such a crash.
CSCud89478	**Symptoms**: Incident report generated ACR: b2bcontentprocessorevent Line: 42. **Workaround**: The Ivy process is automatically restarted so there is a limited impact.
CSCue03851	**Symptoms**: A VCS may become inaccessible from the network and the following log line seen in the kernel logs: kernel: ipv4: Neighbour table overflow. kernel: ipv4: Neighbour table overflow. kernel: net_ratelimit: nnn callbacks suppressed **Conditions**: This may be seen on very large networks when the VCS internal ARP cache size becomes overwhelmed. **Workaround**: Reboot the VCS to clear the ARP cache.
CSCue18609	**Symptom**: The VCS pushes registered provisioned device data to TMS. This data is used by TMS to build user CDRs. If there is any bad data in the device list, there is no way to clear out this table so that TMS can work with good data. The TMS Provisiong Devices page has an option to delete the devices, and the the cleanup option clears out these deleted devices, but when VCS performs a full sync with TMSPE, all of the delete devices return. There should be a way on the VCS to clear the devices table. Or the VCS should honor the deletes performed on the TMS. **Workaround**: None.
CSCue48571	**Symptoms**: Web administration stops functioning. **Conditions**: Time zone configured to use "localtime". **Workaround**: Configure the system with a different time zone.

Table 4: Issues resolved in X8.1 (continued)

Identifier	Description
CSCug34686	**Symptom**: 2833 DTMF events from a video endpoint are not interpreted correctly by an IOS gateway. **Conditions**: Call is originated as H.323 and interworked to SIP by the VCS. **Workaround**: Avoid interworking the call on the VCS.
CSCug56263	**Symptom**: On importing a CPL that includes a rule-switch rule without including the "origin" element, an alarm is raised. This element is described as optional. **Conditions**: The CPL file needs to include a rule-switch element without the "origin" option in order to observe this issue. **Workaround**: Modify the rule-switch element to include a catch all origin statment e.g. <taa:rule origin=".* destination=".*">
CSCuh99358	**Symptom**: Cannot establish a Neighbor Zone when using Dual Interfaces & LAN2 is default route. **Conditions**: The VCS Expressway cannot successfully set up a neighbor zone (and specifically neighbor zone) relationship over SIP to other remote servers (e.g. a remote, 3rd party, VCS, SIP Proxy, etc.) when LAN2 is the NAT interface and the default gateway for the VCS Expressway.
CSCuh49196	**Symptom**: VCS using excess virtual memory as recorded in sensor logs. SNMPD appears to be using excess memory usage. **Conditions**: SNMP configured. **Workaround**: Possibly disable SNMP in the GUI or change SNMP mode to v2c.
CSCuh49320	**Symptoms**: Can’t complete LDAP configuration while selecting SRV record for FQDN address resolution. **Conditions**: Configure LDAP server with SRV record. **Workaround**: Configure LDAP server with address host record or IP address.
CSCuh41614	**Symptom**: VCS reports an application error, and the process restarts automatically. An alarm is raised reporting "An unexpected software error was detected in app[nnnn]: SIGABRT (tkill(2) or tgkill(2))" The incident report associated with this points to a problem in sipparams.cpp:SipParams_setParam:425 **Workaround**: None, the application process is automatically restarted.
CSCui15452	**Symptom**: When dialing out into an external VCS, it sends back a 422 Session Interval Too Small. The VCS should proxy this back to the originator of the call for the originator to send a reINVITE with a bigger Session Refresh. Instead, it seems that the moment the VCS receives the 422 Session Interval Too Small, IWF kicks in instead and attempts to send it out via H.323 which we do not want as we know the number to be a SIP only number. **Conditions**: External VCS with a larger session interval than the local VCS, IWF enabled on local VCS with H.323 and SIP enabled on the affected trunk. **Workaround**: Turn off H.323 on the trunk where this problem is occurring to disable interworking. If H.323 absolutely needs to be on, the min SE on the local VCS may be increased instead to match the min SE of the external VCS. Note that changing the min SE may have repercussions on the network and will require extensive regression testing.

Table 4: Issues resolved in X8.1 (continued)

Identifier	Description
CSCuh78199	**Symptom**: Multiway conference already established between three endpoints (two CUCM and one VCS hosted). An additional CUCM user calls the conference initiator on the VCS but cannot be joined to the conference. **Workaround**: None.
CSCuh98112	**Symptom**: When an endpoint dials to the internet, it sends its private IP to Cisco side in the SDP and hence media fails. When you force the call through the VCS, DNS returns port 5061 and 5060 for cisco.com, however 5061 is disabled on the firewall. It says TCP Connection failed for 5061 and never falls back to TCP. In another test, we disabled TLS on the VCS altogether, in this case the VCS just reports TLS not active and rejects the call with 408 Request timeout. **Conditions**: VCS not falling back to TCP when it cannot establish connection with TLS. **Workaround**: Turn on 5061 on the firewall and enable TLS on VCS.

Open issues

To find the latest information about defects in this release, use the Cisco Bug Search Tool.

Limitations

Unsupported features (general)

- DTLS is not supported through the VCS Control/VCS Expressway; attempts to make secure calls will fail
- SIP Early Media
- SIP KeyPad Markup Language (KPML)
- Audio calls may be licensed as video calls in some circumstances. Calls that are strictly audio-ONLY consume fewer licenses than video calls. However, when audio calls include non-audio channels, such as the iX channel that enables ActiveControl, they are treated as video calls for licensing purposes.

Unsupported Jabber features when using mobile and remote access

- Directory access mechanisms other than UDS
- Certificate provisioning to remote endpoints e.g. CAPF
- File transfer (except when operating in hybrid Webex mode)
- Deskphone control (QBE/CTI)
- Additional mobility features including DVO-R, GSM handoff and session persistency
- Self-care portal
- Support for Jabber SDK
- Shared lines are supported in a limited way. Multiple endpoints can share a line but in-call features (like hold/resume) only work on the first endpoint that answers. Endpoints sharing the line may not correctly recognise the state of the call.

Unsupported features and limitations when using mobile and remote access

- Secure XMPP traffic between VCS Control and IM&P servers (XMPP traffic is secure between VCS Control and VCS Expressway, and between VCS Expressway and remote endpoint)
- Endpoint management capability (SNMP, SSH/HTTP access)
- Multi-domain and multi-customer support; each VCS deployment supports only one IM&P domain (even though IM & Presence 10.0 or later supports multiple IM&P domains)
- Mobile and remote access functionality is not within the FIPS boundary
- The VCS Control used for Mobile and Remote Access cannot also be used as a Lync 2013 gateway (if required, this must be configured on a stand-alone VCS Control
- NTLM authentication via the HTTP proxy
- Maintenance mode; if a VCS Control or VCS Expressway is placed into maintenance mode, any existing calls passing through that VCS will be dropped
- The VCS Expressway must not have TURN services enabled
- Deployments on Large VM servers are limited to 2500 proxied registrations to Unified CM (the same limit as VCS appliances or equivalent VM)

Supported clients when using mobile and remote access

- Cisco Jabber for Windows 9.7 or later
- Cisco Jabber for iPhone and iPad 9.6.1 or later
- Cisco Jabber for Android 9.6 or later
- Cisco Jabber for Mac 9.6 or later
- Cisco TelePresence endpoints/codecs running TC7.0.1 or later firmware

Interoperability

The interoperability test results for this product are posted to http://www.cisco.com/go/tp-interop, where you can also find interoperability test results for other Cisco TelePresence products.

Updating to X8.2.2

Prerequisites and software dependencies

Existing TMS Agent (legacy mode) provisioning deployments

VCS X8.1 and later no longer supports TMS Agent (legacy mode) provisioning. **Before you upgrade to X8 or later**, if you are using TMS Agent (legacy mode) for provisioning you must first migrate to Cisco TelePresence Management Suite Provisioning Extension which requires TMS 13.2.x. See *Cisco TMS Provisioning Extension Deployment Guide* for instructions about how to migrate.

Existing OCS Relay deployments

VCS X8.1 and later no longer supports OCS Relay integration with Microsoft Lync 2010 / OCS 2007 R2. If you use OCS Relay you must migrate to using the Microsoft Lync B2BUA to route SIP calls between the

VCS and a Microsoft Lync Server. See *VCS and Microsoft Lync Deployment Guide* for information about how to configure your video network.

Existing non-AES build installations

As of version X8.1, the software uses AES encryption. Prior to this, a version that used weaker encryption was available. If you are upgrading to X8.1 or later (or another version that uses AES) from a version that used the weaker encryption, you **must** perform a factory reset. Proceed as follows to ensure you can upgrade in future:

1. Record all your software configuration details
2. Upgrade the software with the AES-encryption version
   All configuration will be lost
3. Perform a factory reset
4. Manually reconfigure the software

Firewall ports configuration changes

See Changes in X8.2.2 [p.2] for important information relating to port changes that may affect your firewall configuration.

Upgrade instructions

- When maintenance mode is enabled on a VCS, existing calls passing through that VCS may be dropped. We recommended that you upgrade VCS components while the system is inactive.
- Early field trial customers who have configured a previous X8.1 or X8.1.1 system for external XMPP federation must reconfigure their XMPP federation settings after upgrading to X8.2.

If you are upgrading a VCS that uses clustering, device provisioning (Cisco TMSPE) or FindMe (with Cisco TMS managing VCS), you must follow the directions in *VCS Cluster Creation and Maintenance Deployment Guide*.

Follow the procedure below for upgrading VCS to X8.2.2, only if all of the following apply:

- The VCS is not part of a cluster
- Device provisioning is not in use
- Cisco TMS is not managing the VCS
- VCS is currently running X5.1.1 or later

To upgrade a VCS:

1. Backup the VCS (**Maintenance > Backup and restore**).
   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.
   If your system was delivered with X6.1 pre-installed, you must make some configuration changes before using the backup process as described in the section below.
2. Enable maintenance mode.
   Log in to the VCS as admin (SSH or serial), and at a command prompt, type:
   `xConfiguration SystemUnit Maintenance Mode: On`
   Note that from X8.1 you can enable maintenance mode via the web interface (**Maintenance > Maintenance mode**).

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 VCS (**Maintenance > Upgrade**).
   Note that when upgrading to a new major release, for example from X7.n to X8.n you need to supply a valid release key as a part of the upgrade process.
   The web browser interface may timeout during the restart process, after the progress bar has reached the end. This may occur if the VCS carries out a disk file system check – which it does approximately once every 30 restarts.

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

Upgrading VCS Control and VCS Expressway systems connected over a traversal zone

We recommend that VCS Control (traversal client) and VCS Expressway (traversal server) systems that are connected over a traversal zone both run the same software version.

However, a traversal zone link to a VCS system that is running the previous major release of VCS software is supported. This means that you do not have to upgrade your VCS Control and VCS Expressway systems simultaneously.

Note that certain features introduced in the most recent software version (such as mobile and remote access) require both the VCS Control and VCS Expressway systems to be running the same software version.

Backing up 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:

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

Upgrading from older releases

You cannot upgrade to X7.n or later from releases prior to X5.1. You must first upgrade to X5.2 and then to X7.n or later. See the X5.2 release notes 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 file:

1. Go to **Maintenance > Language**.
2. Click **Browse** and select the **.tlp** language pack file you want to upload.
3. Click **Install**.
   The selected language pack is then verified and uploaded. This may take several seconds.
4. Repeat steps 2 and 3 for any other languages you want to install.

After upgrading to this software release, if you have previous language packs installed, you will see a "Language pack mismatch" alarm. Updated language packs for this release will be made available soon. In the meantime you will see a mixture of some text in your chosen language and some text (predominantly text related to new features) in English.

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.

Available languages

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

Table 5: Available language packs

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

Port reference

The following tables list the IP ports and protocols used by VCS for general services and functions.

For more information about ports, including those used for Unified Communications, device authentication, and the Microsoft Lync B2BUA see *VCS IP Port Usage for Firewall Traversal*.

The tables show the generic defaults for each service, many of which are configurable. The actual services and ports used on your system will vary depending on its configuration, the option keys installed and features that have been enabled. A specific list of all the IP ports in use on a particular VCS can be viewed via the port usage pages (**Maintenance > Tools > Port usage**).

When Advanced Networking is enabled, all ports configured on the VCS, including those relating to firewall traversal, apply to both IP addresses; you cannot configure ports separately for each IP address.

Local VCS inbound/outbound ports

These are the IP ports on the VCS used to receive (inbound) or send (outbound) communications with other systems.

Table 6: Local inbound/outbound ports

Service/ function	Purpose	VCS port (default)	Direction	Configurable via
SSH	Encrypted command line administration.	22 TCP	inbound	not configurable
HTTP	Unencrypted web administration.	80 TCP	inbound	not configurable
NTP	System time updates (and important for H.235 security).	123 UDP	outbound	not configurable
SNMP	Network management.	161 UDP	inbound	not configurable
HTTPS	Encrypted web administration.	443 TCP	inbound	not configurable
Clustering	IPsec secure communication between cluster peers.	500 UDP	inbound outbound	not configurable
Clustering	IPsec secure communication between cluster peers.	IP protocol 51 (IPSec AH)	inbound outbound	not configurable
Reserved		636	inbound	not configurable
DNS	Sending requests to DNS servers.	1024 - 65535 UDP	outbound	**System > DNS**
Gatekeeper discovery	Multicast gatekeeper discovery. The VCS does not listen on this port when **H.323 Gatekeeper Auto discover mode** is set to *Off* (this disables IGMP messages).	1718 UDP	inbound	not configurable
H.323 registration Clustering	Listens for inbound H.323 UDP registrations. If the VCS is part of a cluster, this port is used for inbound and outbound communication with peers, even if H.323 is disabled.	1719 UDP	inbound outbound	**Configuration > Protocols > H.323**
H.323 call signaling	Listens for H.323 call signaling.	1720 TCP	inbound	**Configuration > Protocols > H.323**
Assent call signaling	Assent signaling on the VCS Expressway.	2776 TCP	inbound	**Configuration > Traversal > Ports**
H.460.18 call signaling	H.460.18 signaling on the VCS Expressway.	2777 TCP	inbound	**Configuration > Traversal > Ports**
Traversal server media demultiplexing RTP/RTCP	Optionally used on the VCS Expressway for demultiplexing RTP/RTCP media on Small/Medium systems only.	2776/2777 UDP	inbound outbound	**Configuration > Traversal > Ports**
TURN services	Listening port for TURN relay requests on VCS Expressway.	3478 UDP *	inbound	**Configuration > Traversal > TURN**

Table 6: Local inbound/outbound ports (continued)

Service/ function	Purpose	VCS port (default)	Direction	Configurable via
System database	Encrypted administration connector to the VCS system database.	4444 TCP	inbound	not configurable
SIP UDP	Listens for incoming SIP UDP calls.	5060 UDP	inbound outbound	**Configuration > Protocols > SIP**
SIP TCP	Listens for incoming SIP TCP calls.	5060 TCP	inbound	**Configuration > Protocols > SIP**
SIP TLS	Listens for incoming SIP TLS calls.	5061 TCP	inbound	**Configuration > Protocols > SIP**
B2BUA	Internal ports used by the B2BUA. Traffic sent to these ports is blocked automatically by the VCS's non-configurable firewall rules.	5071, 5073 TCP	inbound	not configurable
Traversal server zone H.323 Port	Port on the VCS Expressway used for H.323 firewall traversal from a particular traversal client.	6001 UDP, increments by 1 for each new zone	inbound	**Configuration > Zones**
Traversal server zone SIP Port	Port on the VCS Expressway used for SIP firewall traversal from a particular traversal client.	7001 TCP, increments by 1 for each new zone	inbound	**Configuration > Zones**
H.225 and H.245 call signaling port range	Range of ports used for call signaling after a call is established.	15000 - 19999 TCP	inbound outbound	**Configuration > Protocols > H.323**
SIP TCP outbound port range	Range of ports used by outbound TCP/TLS SIP connections to a remote SIP device.	25000 - 29999 TCP	outbound	**Configuration > Protocols > SIP**
Ephemeral ports	Various purposes. (The default range of 30000 – 35999 applies to new installations of X8.1 or later; the previous default range of 40000 – 49999 still applies to earlier releases that have upgraded to X8.1.)	30000 – 35999	outbound	**System > Administration**

Table 6: Local inbound/outbound ports (continued)

Service/ function	Purpose	VCS port (default)	Direction	Configurable via
Multiplexed traversal media (Assent, H.460.19 multiplexed media)	Ports used for multiplexed media in traversal calls. RTP and RTCP media demultiplexing ports are allocated from the start of the traversal media ports range. The default media port range of 36000 to 59999 applies to new installations of X8.1 or later. In Large systems the first 12 ports in the range – 36000 to 36011 – are used for multiplexed traffic only. In Small/Medium systems you can either explicitly specify the 2 ports to use for multiplexed traffic or use the first 2 ports from the media port range. The previous default range of 50000 - 54999 still applies to earlier releases that have upgraded to X8.1 or later.	36000 – 36001 UDP (Small / Medium systems) or 36000 – 36011 UDP (Large systems)	inbound outbound	**Configuration > Local Zone > Traversal Subzone**
Non-multiplexed media port range	Range of ports used for non-multiplexed media. Ports are allocated from this range in pairs, with the first port number of each pair being an even number. The default media port range of 36000 to 59999 applies to new installations of X8.1 or later. In Large systems the first 12 ports in the range – 36000 to 36011 – are used for multiplexed traffic only. In Small/Medium systems you can either explicitly specify the 2 ports to use for multiplexed traffic or use the first 2 ports from the media port range. The previous default range of 50000 - 54999 still applies to earlier releases that have upgraded to X8.1 or later.	36002 – 59999 UDP (Small / Medium systems) or 36012 – 59999 UDP (Large systems)	inbound outbound	**Configuration > Local Zone > Traversal Subzone**
TURN relay media port range	Range of ports available for TURN media relay.	24000 – 29999 UDP **	inbound outbound	**Configuration > Traversal > TURN**

Note that two services or functions cannot share the same port and protocol; an alarm will be raised if you attempt to change an existing port or range and it conflicts with another service.

* On Large systems you can configure a range of TURN request listening ports. The default range is 3478 – 3483.

** The default TURN relay media port range of 24000 – 29999 applies to new installations of X8.1 or later. The previous default range of 60000 – 61799 still applies to earlier releases that have upgraded to X8.1.

Remote listening ports

These tables show the default listening (destination) ports on the remote systems with which the VCS communicates.

The source port on the VCS for all of these communications is assigned from the VCS's ephemeral range.

Table 7: Remote listening ports

Service/ function	Purpose	Destination port (default)	Configurable via
DNS	Requests to a DNS server.	53 UDP	**System > DNS**
External manager	Outbound connection to an external manager, for example Cisco TMS.	80 TCP	**System > External manager**
NTP	System time updates.	123 UDP	**System > Time**
LDAP account authentication	LDAP queries for login account authentication.	389 / 636 TCP	**Users > LDAP configuration**
TMS Provisioning Extension	Connection to Cisco TMSPE services.	443 TCP	**System > TMS Provisioning Extension services**
Incident reporting	Sending application failure details.	443 TCP	**Maintenance > Diagnostics > Incident reporting > Configuration**
Third-party FindMe / User Policy server	Outbound connection to a third-party FindMe / User Policy server.	443 TCP	**Applications > FindMe**
Remote logging	Sending messages to the remote syslog server.	514 UDP 6514 TCP	**Maintenance > Logging**
Neighbors (H.323)	H.323 connection to a neighbor zone.	1710 UDP	**Configuration > Zones**
Neighbors (SIP)	SIP connection to a neighbor zone.	5060 / 5061 TCP	**Configuration > Zones**
Traversal zone (H.323)	H.323 connection to a traversal server.	6001 UDP	**Configuration > Zones**
Traversal zone (SIP)	SIP connection to a traversal server.	7001 TCP	**Configuration > Zones**
Endpoint (H.323)	Endpoint listening port	1720 TCP	Defined by endpoint's registration
Endpoint (SIP)	Endpoint listening port	5060 / 5061 TCP / UDP	Defined by endpoint's registration
TURN media relay	Range of ports available for TURN media relay.	24000 – 29999 UDP **	**Configuration > Traversal > TURN** (on VCS Expressway)

** The default TURN relay media port range of 24000 – 29999 applies to new installations of X8.1 or later. The previous default range of 60000 – 61799 still applies to earlier releases that have upgraded to X8.1.

Additional information

Software filenames

The VCS software filenames are in the format s42700x<y_y_y> where x<y_y_y> represents the software version (for example x8_1_0 represents X8.1).

As from X8.1, only AES encrypted software builds are available.

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 *VCS Certificate Creation and Use Deployment Guide* for more information about to how to generate certificate signing requests and install certificates.

Hardware shutdown procedure

The VCS uses a hard drive for storing logs. We recommend that you shut down the appliance prior to it being unplugged to ensure a clean shutdown process. This can be done from the web interface.

Network support

The 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 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.

We recommend that speed and duplex settings are set to auto unless the Ethernet switch that the VCS is connected to does not support auto-negotiation; if manually configured, ensure that full duplex is selected.

Restricting access to ISDN gateways (toll-fraud prevention)

VCS Expressway users should take appropriate action to restrict unauthorized access to ISDN gateway resources. See *VCS Basic Configuration (Control with Expressway) Deployment Guide* for information about how to do this.

Supported RFCs

The following RFCs are supported within the VCS X8.2.2 release:

Table 8: Supported RFCs

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

Table 8: Supported RFCs (continued)

RFC	Description
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)
2833	RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
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
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
4479	A Data Model for Presence

Table 8: Supported RFCs (continued)

RFC	Description
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

Initial installation

Initial configuration of the VCS IP address, subnet and gateway can be accomplished through the installation wizard via the serial port or through the front LCD panel. See *Cisco TelePresence Video Communication Server Getting Started*.

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 capacity 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 *VCS on Virtual Machine Installation Guide* for full installation instructions.

Third-party software

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.

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:

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.

Technical support

If you cannot find the answer you need in the documentation, check the website at 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.

To view a list of Cisco TelePresence products that are no longer being sold and might not be supported, visit: www.cisco.com/en/US/products/prod_end_of_life.html and scroll down to the TelePresence section.

Document revision history

Date	Revision	Description
October 2014	08	X8.2.2 maintenance release.
August 2014	07	Note about NAT reflection added to X8.2 changed behavior, republished for X8.2.1.

Date	Revision	Description
August 2014	06	Note about NAT reflection added to X8.2 changed behavior, republished for X8.2.
July 2014	05	X8.2.1 maintenance release.
June 2014	04	X8.2 initial release.
July 2014	03	X8.1.1 release notes republished to include CSCup02323 and advice about upgrading from non-AES encryption builds.
April 2014	02	X8.1.1 maintenance release, including mobile and remote access features.
December 2013	01	X8.1 initial release. [Revised April 2014 to include issue CSCum90139.]

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.