Cisco TelePresence Video Communication Server X8.8.3

Release Notes

First Published: June 2016

Last Updated: January 2017

Contents

Preface

Change History

Table 1 Release Notes Change History

Date	Change	Reason
January 2017	Updated with new notable issue. Update only affects certain deployments that include a VCS or Expressway running version X8.7n software.	CSCvc47502 and CSCvc34689
October 2016	Added list of X8.8.3 enhancements and updated lists of open / resolved issues.	X8.8.3 maintenance release
September 2016	Added list of X8.8.2 enhancements and updated lists of open / resolved issues.	X8.8.2 maintenance release
August 2016	Improved upgrade warning with reverse DNS required for Cisco VCS Expressway.	Customer impact of X8.8 security improvement
August 2016	Terminology corrected.	Document errata
July 2016	Clarify scope of software support on old VCS hardware platform.	Unclear documentation
July 2016	Updated lists of open / resolved issues.	X8.8.1 maintenance release
July 2016	Updated with new notable issue.	CSCva36208
June 2016	First publication.	X8.8 release

Supported Platforms

Table 2 Cisco VCS Software Versions Supported by Platform

Platform name	Serial Numbers	Scope of software version support
Cisco VCS appliance (1st generation)	52A0#####	All features in versions up to and including X8.6.1. Critical fixes only in X8.7.n*. No support for X8.8 or later versions on this hardware.
Cisco VCS appliance (1st generation)	52A1#####-52A4#####	All features in versions up to and including X8.6.1. Critical fixes only in later versions, up to and including X8.8.3*. No support for any versions after X8.8.3 on this hardware.
Small VM (OVA)	(Auto-generated)	X8.1 onwards

Table 2 Cisco VCS Software Versions Supported by Platform (continued)

Platform name	Serial Numbers	Scope of software version support
Medium VM (OVA)	(Auto-generated)	X8.1 onwards
Large VM (OVA)	(Auto-generated)	X8.1 onwards
CE500[†] (Cisco VCS pre-installed on UCS C220 M3L)	52C#####	X8.1.1 onwards
CE1000[†] (Cisco VCS pre-installed on UCS C220 M3L)	52B#####	X8.1.1 onwards
CE1100 (Cisco VCS pre-installed on UCS C220 M4L)	52D#####	X8.6.1 onwards

* As of 12th September 2015, we are not obliged to release new software for these platforms (see End-of-Life Announcement). X8.6.1 is the last version on which you will receive support for all the features included in the software. However, we may encourage you to upgrade to later releases to address critical issues (for example, security vulnerabilities). In this case, we will not support any of the newer features in those releases on these legacy platforms. Ask your Cisco representative about migrating to a newer platform.

† As of 26th February 2016, you cannot order the CE500 and CE1000 appliances from Cisco. See the End-of-sale announcement for other important dates in the lifecycle of these platforms.

Product Documentation

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

For installing the Cisco VCS, see:

- *Cisco VCS Virtual Machine Installation Guide* on the VCS installation guides page.
- *Cisco Video Communication Server CE1100 Appliance Installation Guide* on the VCS installation guides page.

For general administration topics, reference, and maintenance, see:

- *Cisco TelePresence VCS Administrator Guide* in Cisco TelePresence VCS Maintain and Operate Guides
- *Cisco TelePresence VCS Serviceability Guide* in Cisco TelePresence VCS Maintain and Operate Guides

Other documents that may be relevant in your environment:

- Registrar:

  See *Cisco Single VCS Control - Basic Configuration Deployment Guide* on the VCS configuration guides page.
- Firewall Traversal:

  See *Cisco TelePresence VCS Basic Configuration (Control with Expressway) Deployment Guide* on the VCS configuration guides page.
- Cisco Spark: Hybrid services knowledge base
- Clustering:

  See the *Cisco VCS Cluster Creation and Maintenance Deployment Guide*, for your version, at the Cisco TelePresence Video Communication Server (VCS) Configuration Guides page.
- Certificates:

  See *Cisco VCS Certificate Creation and Use Deployment Guide* on the VCS configuration guides page.
- Unified Communications:

  See *Mobile and Remote Access Through Cisco Video Communication Server* on the VCS configuration guides page.

- Cisco Meeting Server:

  See *Cisco VCS with Cisco Meeting Server Deployment Guide* on the VCS configuration guides page.

  Cisco Meeting Server configuration guides page

  See *Cisco Meeting Server API Reference Guide* on the Cisco Meeting Server programming guides page.
- Microsoft Infrastructure:

  See *Cisco VCS and Microsoft Infrastructure Deployment Guide* on the VCS configuration guides page.

Changes in X8.8.3

X8.8.3 is a maintenance release. The lists of Open and Resolved Issues, page 14, have been updated, and the software has the following enhancements:

- The Cisco VCS has been updated to match the leap second adjustment to UTC time.
- The Cisco VCS has also been updated to match the recent change to the TRT (Turkey Time) time zone.

The list of unsupported endpoint features when using Mobile and Remote Access has also been updated.

Changes in X8.8.2

X8.8.2 is a maintenance release. The lists of Open and Resolved Issues, page 14, have been updated, and the software has the following enhancements:

- The call policy rule editor now has more granular control. You can use the web interface to create policy rules to allow or reject calls from specific zones or callers. You can also choose whether the rule applies to authenticated or unauthenticated callers.
- The clustering page now gives better feedback on DNS resolution and peer certificate status during cluster configuration.
- Zone pages now show how many registrations were proxied by the zones.
- The online help has been updated.

Changes in X8.8.1

X8.8.1 is a maintenance release. There are no new features, but the lists of Open and Resolved Issues, page 14, have been updated.

- Cisco Expressway Series has been certified FIPS compliant.
- Several important bug fixes and security patches have been applied.
- The online help has been updated for Expressway registrations and MRA allow list features.

Features in X8.8

Table 3 Feature History by Release Number

Feature / change	X8.8
Skype for Business 2016 and Skype for Business Mobile Support	Supported
Broker for Microsoft SIP Traffic	Supported
Multistream Support	Supported
Service Setup Wizard	Supported
MRA Allow List Improvement	Supported
API for Remote Configuration of MRA	Supported
Large VM CPU Reservation Reduced	Supported
High Security Environment	Supported

Table 3 Feature History by Release Number (continued)

Feature / change	X8.8
Software Package Signing	Supported
SSL/TLS Support Restricted	Supported
Changes and Minor Enhancements	Supported

Skype for Business 2016 and Skype for Business Mobile Support

We have updated our support for Microsoft client and server combinations. The Gateway Cisco VCS deployment is now interoperable with the following Microsoft collaboration products:

Table 4 Lync and Skype for Business Support Introduced in X8.8.3

Clients	On Lync Server 2013	On Skype for Business Server 2015
Skype for Business 2016 (Windows desktop)	Supported	Supported
Skype for Business 2015 (Windows desktop)	Supported	Supported
Skype for Business for iOS	Not supported	Limited support*
Skype for Business for Android	Not supported	Limited support*. See CSCva18731.

* We do not support these clients in calls to MCU bridges. We do support them in other call scenarios, including calls to TelePresence Server bridges.

Broker for Microsoft SIP Traffic

In some previous versions of our *Cisco VCS and Microsoft Interoperability Deployment Guide*, we published an appendix describing how to get Lync to Jabber messaging working using CPL on a "directory VCS".

In X8.8, we have improved that deployment by creating an independent broker to perform the task of filtering and redirecting the messaging and presence traffic coming from the Microsoft infrastructure. This change has the following benefits:

- Maintains the robustness of the SDP parser, by not requiring it to process the non-standard SIP from Microsoft infrastructure
- No requirement for a directory Cisco VCS, because the broker is hosted on the Gateway Cisco VCS.
- The broker is abstracted from the rest of the software so you can disable it if you don't need it.
- If you were using the CPL deployment, you can now upgrade to X8.8 and benefit from the other features and improvements since X8.6.

See *Cisco VCS and Microsoft Infrastructure Deployment Guide* on the VCS configuration guides page.

Multistream Support

The Cisco VCS now supports passthrough of encrypted and unencrypted multistream calls. It also supports passthrough of the encrypted iX protocol required for the ActiveControl feature used by endpoints interacting with the TelePresence Server.

There is a new "Multistream mode" on all zone types that can potentially handle media. The mode is enabled by default, but it only applies when the zone passes media to or from the back to back user agent. The signaling of multistream calls is always passed through, irrespective of the zone's multistream mode setting.

Note:

- The Cisco VCS does not encrypt the iX protocol on behalf of other entities; iX must either be encrypted from end to end, with the endpoints and TelePresence Server doing the encryption, or it must be unencrypted from end to end.

Service Setup Wizard

The Cisco VCS can be used in different ways, some of which do not work together. Version X8.8 improves the user experience of configuring the Cisco VCS for its chosen purpose in your environment.

When you first launch the user interface, you see a Service Setup Wizard instead of going straight into the menu. You can select the system series (VCS or Expressway) and type (*VCS Expressway*/*VCS Control* or *Expressway-E*/*Expressway-C*). These choices affect the list of services available.

Then you select from a number of popular Cisco VCS services:

- Cisco Spark Hybrid Services
- Mobile and Remote Access
- Jabber Guest Services
- Microsoft Interoperability
- Registrar/ Proxy registrations (previously only possible on VCS, now also possible on Expressway)
- Collaboration Meeting Rooms (CMR) Cloud
- Business to Business Calling

When you have selected from the list, the wizard helps you to apply appropriate licenses for your selection, verify your basic configuration (network settings should have been configured previously), and then restart the system.

Following the restart, you'll only see the configuration pages and fields that are relevant for the service you selected. If you don't want to use the wizard you can skip through it, or you can go back to the start at any time.

Table 5 Services That Can Be Hosted Together

	Cisco Spark Hybrid Services (Connectors)	Mobile and Remote Access	Jabber Guest Services	Microsoft Interoperability	Registrar	CMR Cloud	Business to Business calling
Cisco Spark Hybrid Services (Connectors)	Y	N	N	N	N	N	N
Mobile and Remote Access	N	Y	N	N	Y	Y	Y
Jabber Guest Services	N	N	Y	N	Y	Y	Y
Microsoft Interoperability	N	N	N	Y	N	N	N
Registrar	N	Y	Y	N	Y	Y	Y
CMR Cloud	N	Y	Y	N	Y	Y	Y
Business to Business calling	N	Y	Y	N	Y	Y	Y

Key to Table

Y: Yes, these services can be hosted on the same system or cluster

N: No, these services may not be hosted on the same system or cluster

Rules

- Hybrid Services requires a dedicated Expressway-C to host Connectors
- Microsoft Interoperability requires a dedicated VCS Control or Expressway-C (called Gateway VCS or Gateway Expressway in the help and documentation)
- Jabber Guest cannot work with MRA (technical limitation)
- MRA is currently not supported in IPv6 only mode. If you want IPv6 B2B calling to co-reside with IPv4 MRA on the same Cisco VCS traversal pair, the Cisco VCS Expressway and Cisco VCS Control must both be in dual stack mode.

MRA Allow List Improvements

The MRA allow list feature is more specific in this release. When you add, discover, or refresh the Unified Communications nodes on the Cisco VCS Control, the Cisco VCS automatically adds the nodes to the allow list. We are now being a lot more specific by including the port and request path in the allow list rule.

We also improved the interface for manually adding rules, enabling you to accurately specify the URL and so restrict the scope of access. For example, instead of allowing `something.example.com`, now you can add `https://something.example.com:8443/pathto/resource.htm` instead.

You can also restrict which HTTP methods you allow for each of your rules.

Note: You should review your editable rules after you upgrade the Cisco VCS Controls in your MRA deployment. We advise this because any servers you previously added to the allow list are upgraded to prefix matching rules. These rules allow any path on that server, using the default ports for the originally entered protocol.

The automatically added entries are automatically upgraded to be more specific than in previous releases.

API for Remote Configuration of MRA

The Cisco VCS has a new API to simplify remote configuration. Third party systems, such as Cisco Prime Collaboration Provisioning, can use the API to configure Mobile and Remote Access on the Cisco VCS.

The API is self-documented using REST API Markup Language (RAML).

See *Cisco Video Communication Server REST API Reference Guide* on the VCS configuration guides page.

Large VM CPU Reservation Reduced

The Large Cisco VCS VM CPU reservation requirement has been reduced from 25600 MHz to 16000 MHz. This means that two Large Cisco VCS VMs can now comfortably co-reside on a UCS server with two eight-core 3.2 GHz processors, when hyperthreading is enabled. This was not previously possible because the higher reservation requirement, added to the CPU requirement for the hypervisor, exceeded the total processing power of the host.

The new reservation does not limit the maximum Cisco VCS CPU speed; the Cisco VCS can use the headroom provided by the higher specification host.

Security Improvements

High Security Environments

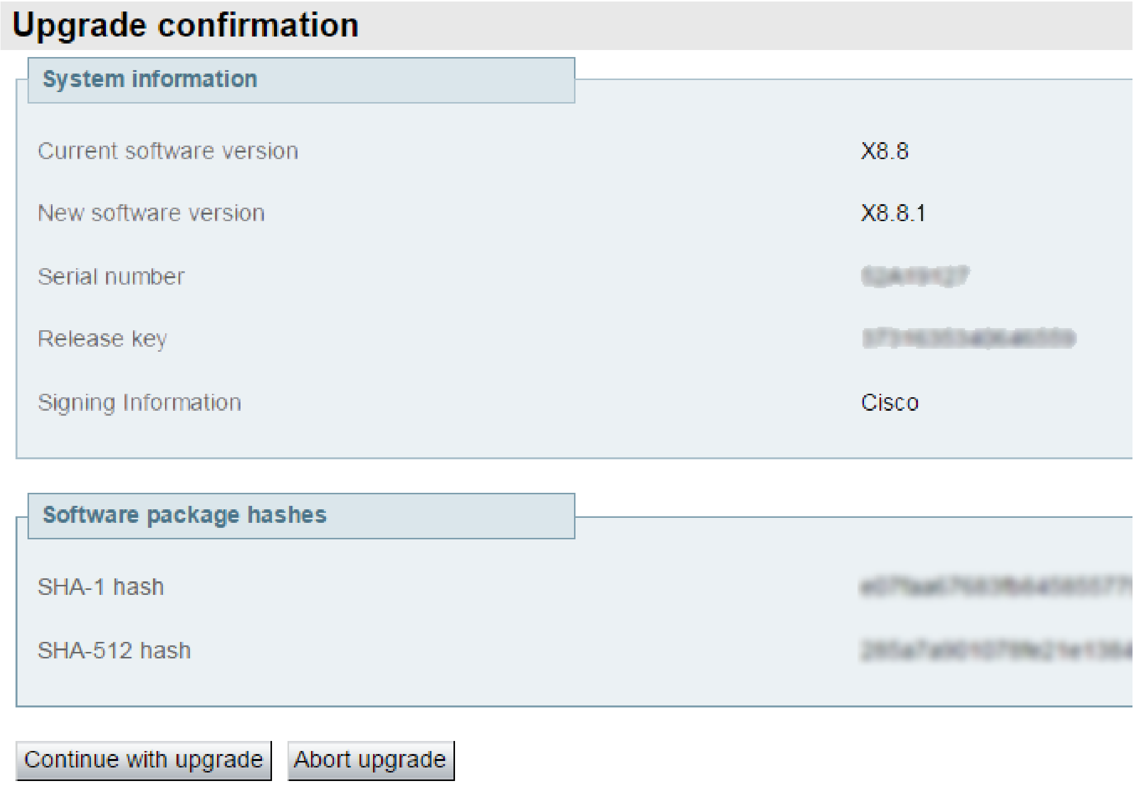
With this release we have improved security in a number of Cisco VCS components, and have implemented new ways of testing and threat modelling, as part of an ongoing effort to improve security.

If you deploy Cisco VCS into a high security environment, you must apply the *Advanced Account Security* option key, then enable **FIPS140-2 cryptographic mode** and acknowledge that you consent to the associated restrictions.

Software Package Signing

Starting with this release, we are signing Cisco VCS software packages to give you confidence in their integrity and authenticity.

We now do an integrity check before you commit to an upgrade. This means you can't tell that the package is being verified on this particular upgrade, because your pre-upgrade version does not have this feature. During your next upgrade, you'll see package signing information, like this:



Upgrade confirmation

System information

Current software version	X8.8
New software version	X8.8.1
Serial number	[redacted]
Release key	[redacted]
Signing Information	Cisco

Software package hashes

SHA-1 hash	[redacted]
SHA-512 hash	[redacted]

TLS Support Restricted

To improve security, the Cisco VCS now only supports specific versions of TLS. The Cisco VCS offers and accepts TLS versions 1.0, 1.1, and 1.2, when establishing secure connections.

Changes and Minor Enhancements

- The Cisco VCS now has a mechanism to reply to all H.323 requests (eg. RRQ) with the request in progress message (RIP). This prevents the requests from timing out, which is possible when an external authentication mechanism does not respond in a timely fashion.

  Use the command `xconfig H323 Gatekeeper Registration RIPAllRequests: On` to enable this feature.
- From version X8.8 onwards, the Cisco VCS does not create DSA host keys. It creates RSA or ECDSA keys instead, for improved security.

  If you upgrade a system that already has a DSA host key, the existing key will persist so that SSH client users do not have to verify the fingerprint again.
- From version X8.8 onwards, connections between cluster peers use TLS instead of IPSec. When you upgrade a cluster, the cluster comes up in TLS permissive mode.
- Multiple Device Messaging (a new feature in IM and Presence Service 11.5) is now supported for clients that connect through Cisco VCS to IM and Presence Service in the cloud.

  This feature is not supported through any versions of Cisco VCS before X8.8.

Open and Resolved Issues

Follow the links below to read the most recent information about the open and resolved issues in this release.

- All open issues, sorted by date modified (recent first)
- Issues resolved by X8.8.3
- Issues resolved by X8.8.2
- Issues resolved by X8.8.1
- Issues resolved by X8.8

Notable Issues in this Version

CSCva18731: **Calls to/from Skype for Business Android v6.4.0.5 fail due to ICE (internal/external)**

Skype for Business for Android version 6.4.0.5 cannot make or receive calls with standards-based endpoints (via Cisco VCS configured for Microsoft interoperability) when the calls have both audio and video streams.

You can work around this issue in one of these ways:

- Using Skype for Business for Android 6.4.0.5 (or later): Make or answer calls as audio-only, and then add video after the audio call is established.
- Use an earlier release of Skype for Business for Android: For example, versions 6.0.0.8, 6.2.0.3, or 6.3.0.2 do not have this issue. Note that these versions are no longer available through the official channels.

CSCvc47502 and CSCvc34689: **Cisco VCS B2BUA drops some RTCP multistreaming Refresh packets during decryption in Cisco WebEx calls**

Note: This software version is only vulnerable to this issue **if** the other end of the call involves a VCS or Expressway running X8.7*x* or earlier.

This issue affects certain TelePresence configurations with Cisco VCS or Cisco Expressway software versions X8.7x.

Affected components

- Cisco TelePresence IX5000 Series immersive endpoint (all versions)
- Cisco VCS or Cisco Expressway versions X8.7.x and earlier
- Cisco TelePresence Server versions 4.3, 4.4(1.9), 4.2 or earlier
- Cisco TelePresence Server versions 4.4(1.16) or later
- Cisco TelePresence TX9000 Series
- Cisco TelePresence System (CTS)
- Other video endpoints

Description

The issue affects calls from immersive TelePresence systems operating in TIP/MUX mode, or other TelePresence systems operating in multistreaming mode. When encrypted/decrypted by VCS or Expressway X8.7.x. The symptoms are pixelated video which gets progressively worse. Then the endpoint terminates the call (because problems with decoding received media lead to perceived packet loss). Other video and quality issues may also occur.

With the TelePresence Server, the following behavior may trigger the issue:

- Versions 4.3 or 4.4(1.9): sharing for more than the session refresh.
- Versions 4.2 or earlier, or 4.4(1.16) or later: starting and stopping sharing multiple times.

Note: This issue does not occur if any of the following cases apply:

- Encryption to / from the VCS / Expressway is disabled.
- TIP/MUX is disabled (immersive systems).
- Multistream is disabled.
- If Cisco WebEx is involved, and WebEx video callback (Call My Video System) is used.

Background

The mechanism for session state maintenance in X8.7.x is susceptible to issues when a high number of SSRC IDs are present in encrypted calls. These include calls from immersive endpoints that use TIP, or from endpoints operating in multistream mode. This issue was resolved by Cisco VCS X8.8.x and later. However, this issue can affect encrypted calls where one of the VCS / Expressways at either end of the call leg is still on X8.7.x while the other is on X8.8.x or later.

Recommendation - Upgrade X8.7.x systems

The CMR Cloud infrastructure (Cisco WebEx) was upgraded from X8.7 to resolve the issue for customers that have VCS or Expressway X8.8.x on-premises. This means that other customers using CMR Hybrid, who have VCS / Expressway X8.7.x on-premises, could now see this issue. We strongly recommend that you upgrade your Cisco VCS / Expressway X8.7.x if you are using multistream/immersive endpoints for encrypted calls with other Cisco infrastructure, like CMR Cloud or third-party partners.

Limitations

Unsupported Features (General)

- DTLS is not supported through the Cisco VCS Control/Cisco VCS Expressway. SRTP is used to secure calls instead; attempts to make DTLS calls will fail.
- SIP UPDATE method. Features that rely on the SIP UPDATE method (RFC 3311) will not work as expected because the Cisco VCS does not support this method.
- 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 Endpoint Features When Using Mobile and Remote Access

Note: This list contains known limitations and is not exhaustive. The MRA deployment does not necessarily support pass through of line-side features provided by Cisco Unified Communications Manager. Absence of such items from this list does not imply that they are supported.

- Call recording for Cisco Jabber endpoints connected over Mobile and Remote Access (MRA).
- Calls to/from additional lines on IP phones and endpoints that support multiple lines; only the primary line is supported via MRA.
- Directory access mechanisms other than UDS.
- Certificate provisioning to remote endpoints e.g. CAPF.
- Features that rely on the SIP UPDATE method (RFC 3311) will not work as expected because the Cisco VCS does not support this method. For example, CUCM and endpoints use UPDATE to implement blind transfer, which does not work correctly via MRA.
- Peer-to-peer file transfer when using IM and Presence Service and Jabber is unsupported via MRA
  - Managed File Transfer (MFT) with IM and Presence Service 10.5.2 (and later) and Jabber 10.6 (and later) clients is supported via MRA
  - File transfer with WebEx Messenger Service and Cisco Jabber is supported via MRA

- Jabber SDK, Jabber for Mac, and Jabber for Windows are not capable of deskphone control when they are connected over MRA, because the CTI-QBE protocol is not traversed by the Cisco VCS pair. When these Jabber applications, or other CTI applications, can connect to CUCM CTIManager (on-premises or VPN) then they can deskphone control endpoints and clients that are connected over MRA.
- Additional mobility features including GSM handoff and session persistency.
- Hunt group/hunt pilot/hunt list.
- Self-care portal.
- Support for Jabber SDK.
- Shared lines are not supported on endpoints connected over MRA.

  Some shared line features may work but are not supported.

Unsupported Cisco VCS Features and Limitations When Using Mobile and Remote Access

- The Cisco VCS cannot be used for Jabber Guest when it is used for MRA.
- The Cisco VCS Control used for Mobile and Remote Access cannot also be used for Microsoft Interoperability. Microsoft Interoperability requires a dedicated Cisco VCS Control.
- MRA is not supported in IPv6 only mode.
- Endpoint management capability (SNMP, SSH/HTTP access).
- Multi-domain and multi-customer support is limited as follows:
  - Prior to X8.5, each Cisco VCS deployment supported only one IM&P domain (even though IM and Presence Service 10.0 or later supports Multiple Presence Domains).
  - As of X8.5, you can create multiple deployments on the Cisco VCS Control, but this feature is still limited to one domain per deployment.
  - As of X8.5.1, a deployment can have Multiple Presence Domains. This feature is in preview, and we currently recommend that you do not exceed 50 domains.
- NTLM authentication via the HTTP proxy.
- Maintenance mode; if the Cisco VCS Control or the Cisco VCS Expressway is placed into maintenance mode, any existing calls passing through that Cisco VCS will be dropped.
- The Cisco 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 Cisco VCS appliances or equivalent VM).

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.

Notable Interoperability Concerns

X8.7.n (and earlier versions) of Cisco VCS are not interoperable with Cisco Unified Communications Manager IM and Presence Service 11.5(1).

This is caused by a deliberate change in that version of IM and Presence Service, and there is a corresponding change in Cisco VCS X8.8.

To ensure continuous interoperability, you must upgrade your Cisco VCS systems to X8.8 *before* you upgrade your IM and Presence Service systems to 11.5(1).

The symptom of the issue is an error on Cisco VCS as follows:

```
Failed Unable to Communicate with <IM&P node address>. AXL query HTTP error "'HTTPError:500'"
```

Upgrading to X8.8.3

Prerequisites and Software Dependencies

Upgrade Caution, PLEASE READ: X8.8 is more secure than earlier versions. Upgrading could cause your deployments to stop working as expected, so you must check for the following environmental issues before you upgrade to X8.8:

- Minimum versions of Unified Communications infrastructure: Some versions of Unified CM, IM and Presence Service, and Cisco Unity Connection have been patched with CiscoSSL updates. Check that you're running the minimum versions described in the Mobile and Remote Access deployment guide, before you upgrade Cisco VCS to X8.8.

  See *Mobile and Remote Access Through Cisco Video Communication Server* on the VCS configuration guides page.

  IM and Presence Service 11.5 is an exception. You must upgrade Cisco VCS to X8.8 before you upgrade IM and Presence Service to 11.5.
- Certificates: Certificate validation has been tightened up in X8.8.
  - Try the secure traversal test before and after upgrade (**Maintenance > Security certificates > Secure traversal test**) to validate TLS connections.
  - Are your Unified Communications nodes using valid certificates that were issued by a CA in the Cisco VCS Controls' trust list?
  - If you are using self-signed certificates, are they unique? Does the trusted CA list on Cisco VCS have the self-signed certificates of all the nodes in your deployment?
  - Are all entries in the Cisco VCS's trusted CA list unique? You must remove any duplicates.
  - If you have TLS verify enabled on connections to other infrastructure (always on by default for Unified Communications traversal zone, and optional for zones to Unified Communications nodes) you must ensure that the hostname is present in the CN or SAN field of the host's certificate. We do not recommend disabling TLS verify mode, even though it may be a quick way to resolve a failing deployment.
- DNS entries: Do you have forward and reverse DNS lookups for all infrastructure systems that the Cisco VCS interacts with?

  Important! From version X8.8, you must create forward and reverse DNS entries for all Cisco VCS Expressway systems, so that systems making TLS connections to them can resolve their FQDNs and validate their certificates.

  If the Cisco VCS cannot resolve hostnames and IP addresses of systems, your complex deployments (eg. MRA) could stop working as expected after you upgrade.
- Cluster peers: Do they have valid certificates? If they are using default certificates you should replace them with (at least) internally generated certificates and update the peers' trust lists with the issuing CA.

  Note: If you are upgrading to X8.8 or later from an earlier version, clustering communications changed in X8.8 to use TLS connections between peers instead of IPSec. TLS verification is not enforced (by default) after you upgrade, and you'll see an alarm reminding you to enforce TLS verification.

Hybrid Services

Your Management Connector must be up to date before you upgrade your Cisco VCS. You must authorize and accept any upgrades advertised by the Cisco Collaboration Cloud before attempting to upgrade.

Note: X8.7.1 is now the minimum version required for Hybrid Services. If you are using Hybrid Services with X8.7, you must upgrade to X8.7.1 or later.

Existing TMS Agent (Legacy Mode) Provisioning Deployments

Cisco 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

Cisco 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 Interoperability B2BUA to route SIP calls between the Cisco VCS and Microsoft infrastructure. See *Cisco VCS and Microsoft Infrastructure Deployment Guide* for information about this deployment.

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

Upgrade Instructions

We recommend that you upgrade Cisco VCS components while the system has low levels of activity.

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

Follow the procedure below for upgrading Cisco VCS to X8.8.3, only if all of the following apply:

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

To upgrade a Cisco VCS:

1. Backup the Cisco 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 Cisco 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 Cisco 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 Cisco VCS carries out a disk file system check – which it does approximately once every 30 restarts.

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

Upgrade Cisco VCS Control and Cisco VCS Expressway systems connected over a traversal zone

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

However, we do support a traversal zone link from one Cisco VCS system to another that is running the previous major release of Cisco VCS. This means that you do not have to simultaneously upgrade your Cisco VCS Control and Cisco VCS Expressway systems.

Note that certain services (such as Mobile and Remote Access) require both the Cisco VCS Control and Cisco VCS Expressway systems to be running the same software version.

Back up 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:

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.

Upgrade from older releases

- We strongly recommend installing a new server certificate if you are upgrading from any version of Cisco VCS released prior to X8.1.1.
- The certificate signing request storage location changed in X8:
  - When you generate a CSR in X7, the application puts **csr.pem** and **privkey_csr.pem** into **/tandberg/persistent/certs**.
  - When you generate a CSR in X8, the application puts **csr.pem** and **privkey.pem** into **/tandberg/persistent/certs/generated_csr**.

  If you want to upgrade from X7 and have an unsubmitted CSR, then we recommend discarding the CSR before upgrade, and then regenerating the CSR after upgrade.
- 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.

Using Collaboration Solutions Analyzer

Collaboration Solutions Analyzer is a tool created by Cisco Technical Assistance Center (TAC) to help you with troubleshooting, by analyzing log files from your Cisco TelePresence Video Communication Server.

To get started:

1. Collect the logs from your Cisco TelePresence Video Communication Server.
2. Sign in to https://cway.cisco.com/tools/CollaborationSolutionsAnalyzer/.

   (You need a customer or partner account to sign in).
3. Paste or drag in your log file.
4. Click **Run**.

The tool analyzes the log file and displays the information in a format that is much easier to understand than the raw logs. For example, you can generate ladder diagrams to show SIP calls.

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.

Obtaining Documentation and Submitting a Service Request

Use the Cisco Notification Service to create customized flexible notification alerts to be sent to you via email or by RSS feed.

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

Cisco Legal Information

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.

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.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

© 2017 Cisco Systems, Inc. All rights reserved.

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: 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. (1110R)