Cisco TelePresence Video Communication Server X8.9

Release Notes

First Published: December 2016

Last Updated: February 2017

Contents

Preface

Change History

Table 1 Release Notes Change History

Date	Change	Reason
February 2017	Republished with clarification for scope of shared line/ multiple line feature.	Customer found issue.
December 2016	First publication.	X8.9

Supported Platforms

Table 2 Cisco VCS Software Versions Supported by Platform

Platform name	Serial Numbers	Scope of software version support
Small VM (OVA)	(Auto-generated)	X8.1 onwards
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 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.

Some VCS hardware appliances are not supported

We do not support this Cisco VCS software version on the 1st generation Cisco VCS hardware appliances, serial numbers 52A########.

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* on the Cisco TelePresence VCS maintain and operate guides page.
- *Cisco TelePresence VCS Serviceability Guide* on the Cisco TelePresence VCS maintain and operate guides page.

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, on 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.

New Features in X8.9

Table 3 Feature History by Release Number

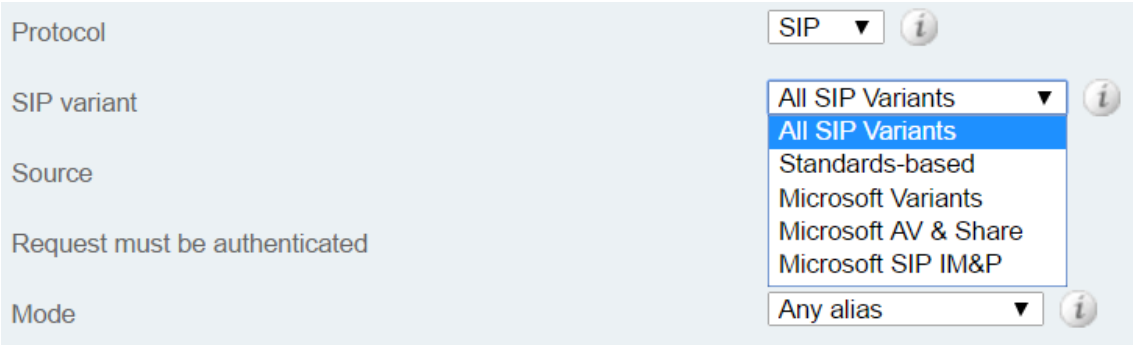
Feature / change	X8.9
Edge Traversal of Microsoft SIP Traffic for Cisco Meeting Server	Supported
Meeting Server Web Proxy	NOT SUPPORTED
IM and Presence Service Federation With Skype for Business or Office 365 Organizations	Preview
REST API Expansion	Supported
Allow Jabber for iPhone and iPad to Use Safari for SSO Over MRA	Supported
Shared Line / Multiple Line Support for MRA Endpoints	Preview
Smart Call Home	Preview
Secure Install Wizard	Supported
DiffServ Code Point Marking	Supported
Maintenance Mode For MRA	Supported
X8.9 Changes and Enhancements	Supported

Edge Traversal Integration with Cisco Meeting Server

The Cisco VCS pair at the edge of the network can now traverse Microsoft SIP traffic to and from Cisco Meeting Server spaces. This enables collaboration in spaces between your users and people from external organizations that use Office 365 or Microsoft Skype for Business infrastructure.

Two Cisco VCS enhancements help you configure these collaboration scenarios:

- The DNS zone can do SRV lookups for the Microsoft federation service (`._sipfederationtls._tcp.example.com.`)
- Search rules now have the ability to route calls based on which variant of SIP is used on the call



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

(Preview) IM and Presence Service Federation With Skype for Business or Office 365 Organizations

The Cisco VCS pair at the edge of the network can now traverse messaging and presence traffic between IM and Presence Service and external organizations using Skype for Business or Office 365.

This feature is in preview as it requires corresponding changes to Cisco Unified Communications Manager IM and Presence Service that are not yet released.

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

REST API Expansion

In X8.8, we introduced a new API to simplify remote configuration. Third party systems, such as Cisco Prime Collaboration Provisioning, can now use the API to configure the following features / services on the Cisco VCS:

- Mobile and Remote Access (MRA)
- Business to business (B2B) calls

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.

Allow Jabber on iOS to Use Safari for SSO Over MRA

This option applies if you use single sign-on (SSO) and have Cisco Jabber iOS endpoints that access Unified Communications services from outside the network. In this case, by default the identity provider's authentication page is displayed in an embedded web browser (not the Safari browser) on the iOS devices. That default browser is unable to access the iOS trust store, and so cannot use any certificates deployed to the devices. From X8.9, you can optionally configure Cisco VCS Expressway to allow Jabber on iOS devices to use the native Safari browser. Because the Safari browser *is* able to access the device trust store, you can now enable password-less authentication or two-factor authentication in your SSO deployment.

Caveat

A potential security issue exists for this option. The mechanism to return browser control from Safari to Jabber after the identity provider authentication completes, uses a custom URL scheme that invokes a custom protocol handler. It's possible that another application other than Jabber could intercept the scheme and gain control from iOS. In that case, the application would have access to the OAuth token in the URL.

If you are confident that your iOS devices will not have other applications that register the Jabber custom URL scheme, for example because all mobile devices are managed, then it's safe to enable the option. If you are concerned about the possibility of another app intercepting the custom Jabber URL, then do **not** enable the embedded Safari browser.

Note: Make sure that you apply this option consistently in Cisco VCS Expressway and in Unified CM. If you decide to enable or disable it in one application, do the same in the other. The relevant settings are:

- **Allow Jabber iOS clients to use embedded Safari browser** in Cisco VCS Expressway (**Configuration > Unified Communications > Configuration > Single Signon** section)
- **SSO Login Behavior for iOS** in Unified CM (**System > Enterprise Parameters > SSO Configuration** section)

Supported endpoints

- Cisco Jabber for iOS 11.8 or later, on devices using iOS 9 or later

Supported Unified Communications services

- Cisco Unified Communications Manager 11.5(1)SU1 or later
- Cisco Unity Connection 11.5(1) or later

(Preview) Shared Line / Multiple Line Support for MRA Endpoints

Cisco VCS now supports pass through of Unified CM shared line and multiple line features for endpoints that are connecting by Mobile and Remote Access.

The benefit of this feature is that remote and mobile endpoint users can use features, like barge, conference barge, hold on one device and resume on another, in the same way as they would when they are on the premises.

You need to configure multiple and shared lines for users and their MRA devices on Unified CM.

Required versions:

- Unified CM 11.5(1)SU2 or later
- Cisco VCS X8.9 or later
- Cisco IP Phone 7800 Series and Cisco IP Phone 8800 Series phones, with firmware version 11.5(1) or later

Note: This feature is disabled by default, because it impacts some features on earlier versions of Unified CM.

If you are using a Unified CM version before 11.5(1)SU2, and you enable SIP Path headers on Cisco VCS Control, the following Unified CM features will *report the MRA devices' IP addresses instead of the Cisco VCS's IP address*:

- Device Mobility
- Real-Time Monitoring Tool (RTMT)
- Cisco Emergency Responder (CER)

Other features may also be affected by this change. The devices' IP addresses are not useful for determining their location, as they are typically from reserved private ranges and could overlap with your organization's internal range.

(Preview) Smart Call Home

Smart Call Home is a free embedded support capability for Cisco VCS. It offers proactive diagnostics and real-time alerts, enabling higher network availability and increased operational efficiency.

Smart Call Home notifies users of Schedule- and Event-based notifications.

- Schedule-based: inventory, telemetry and configuration messages used to generate a Device Report and improve hardware and software quality by identifying failure trends. You can find these notifications posted on the first day of every month.
- Event-based: asynchronous events already supported by Cisco VCS such as alarms and ACRs. You will find these notifications posted to the Smart Call Home server as and when they occur.

You can opt to keep your organization's details anonymous. In this case Cisco VCS sends reports to the Smart Call Home server as normal, but the server does not send out notifications.

Secure Install Wizard

The Cisco VCS now includes an Install Wizard that helps make the deployment and configuration of your system easier and more secure.

The Install Wizard guides you through the initial configuration required to get your system up and running securely. Any further configuration is then possible using the web interface or CLI.

Only the person authorized to complete the system installation can access and complete the initial setup on the system console (or VM equivalent). All accounts on the Cisco VCS are disabled upon first boot until the installation is

complete. The system is also not accessible over the network interface until the installation has been completed and secured.

In a VM deployment, any preconfigured data gets imported when the VM boots for the first time and you are not required to re-enter data.

The Install Wizard does not affect the upgrade procedure for an existing system, as the system maintains any data that you have already configured.

Improved DiffServ Code Point Marking

If you use our Unified Communications Mobile and Remote Access solution, from X8.9 the Cisco VCS supports improved DSCP (Differentiated Service Code Point) packet marking for traffic passing through the firewall. DSCP is a measure of the Quality of Service level of the packet. To provide more granular control of traffic prioritization, DSCP values are set (marked) for these individual traffic types:

Traffic type	Supplied default value	Web UI field
Video	34	QoS Video
Audio	46	QoS Audio
XMPP	24	QoS XMPP
Signaling	24	QoS Signaling

Before X8.9 you had to apply DSCP values to all signaling and media traffic collectively.

You can optionally change the default DSCP values from the **System > Quality of Service** web UI page (or the CLI).

Notes:

- DSCP value "0" specifies standard best-effort service.
- DSCP marking is applied to SIP and H.323 traffic.
- DSCP marking is applied to TURN media, providing the TURN traffic is actually handled by the Cisco VCS.

Existing QoS/DSCP Commands and API are Discontinued

From X8.9 we no longer support the previous methods to specify QoS/DSCP values. The former Web UI settings QoS Mode and QoS Value, CLI commands `xConfiguration IP QoS Mode` and `xConfiguration IP QoS Value` and corresponding API are now discontinued. Do not use these commands.

What if I currently use these commands?

When you upgrade the Cisco VCS, any existing QoS value you have defined is automatically applied to the new fields and replaces the supplied defaults. For example, if you had a value of 20 defined, all four DSCP settings (QoS Audio, QoS Video, QoS XMPP, QoS Signaling) are set to 20 also.

We don't support downgrades. If you need to revert to your pre-upgrade software version, the QoS settings are reset to their original supplied defaults. So QoS Mode is set to *None* and QoS Value is set to *0*. You will need to manually redefine the values you want to use.

Improved Maintenance Mode

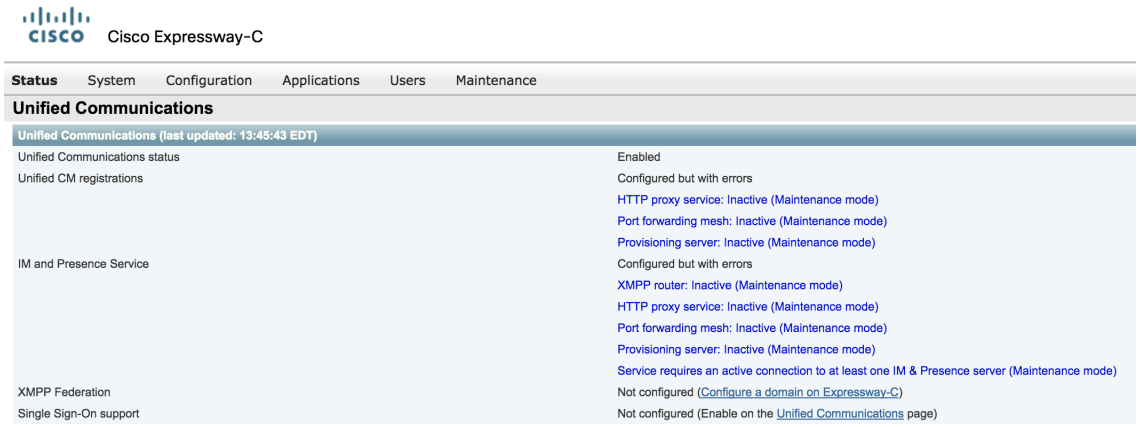
Maintenance mode on the Cisco VCS has been enhanced so that you can bring an MRA system down in a managed way.

When you engage maintenance mode, the Cisco VCS stops accepting new calls or proxy (MRA) traffic. Existing calls and chat sessions are not affected.

As users end their sessions normally, the system comes to a point when it is not processing any traffic of a certain type, and then it shuts that service down.

If users try to make new calls or start new chat sessions while the Cisco VCS is in maintenance mode, the clients will receive a service unavailable response, and they might then choose to use another peer (if they are capable). This fail-over behavior depends on the client, but restarting the client should resolve any connection issues if there are active peers in the cluster.

The Unified Communications status pages also show (Maintenance Mode) in any places where MRA services are affected.



Other Changes and Enhancements

- You can nominate an administrator account as an emergency account. In case the Cisco VCS disallows local authentication but is unable to connect to a remote authentication service.
- We have removed the limitation that TURN services should not be enabled on a system that is being used for MRA. We did this to allow services that require TURN to coexist with MRA. One example is edge traversal for Cisco Meeting Server.

  Note: This change does not make Jabber Guest compatible with MRA. It also does not mean that TURN can be used for MRA. The change simply means that MRA is not impacted if you enable TURN services (for other reasons).
- We have discontinued the pre-X8.9 API and CLI commands for defining QoS/DSCP values: `xConfiguration IP QoS Mode` and `xConfiguration IP QoS Value`. They are replaced by new commands / web UI settings.
- The web administration port is now configurable, on the **System > Administration** page. The default port is still 443.
- From X8.9 onwards, automated intrusion protection is enabled, by default, for the following categories:
  - http-ce-auth
  - http-ce-intrusion
  - sshpfwd-auth
  - sshpfwd-intrusion
  - xmpp-intrusion

  This change affects new systems. Upgraded systems keep their existing protection configuration.

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 X8.9

Notable Issues in this Version

Limitations

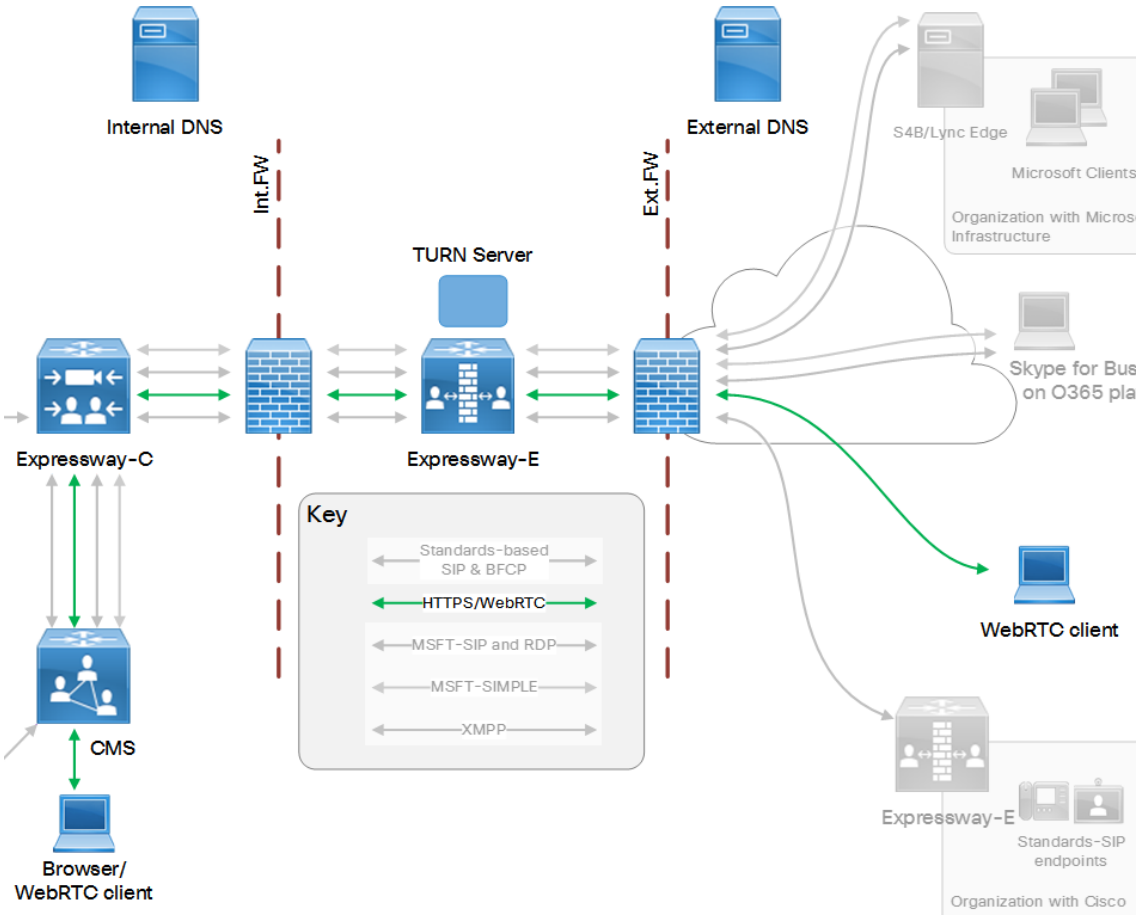
Unsupported Features (General)

- 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 Cisco Meeting Server Web Proxy

CAUTION: Do not use the Meeting Server Web Proxy feature. This feature is not supported with this release of Cisco VCS, due to known issues.

We've added a reverse https proxy for Meeting Server, which enables off-premises users to browse to a Meeting Server Web Bridge. Users can manage or join spaces without having any software other than a supported browser.



The proxy requires very little additional configuration on the Cisco VCS pair; you simply enter the Meeting Server listening address on the Cisco VCS Control, and the pair makes use of the existing traversal connection to proxy external https requests to that address.

You can enable the Meeting Server Web Proxy on the same Cisco VCS pair as MRA or other traversal features, but you cannot use it when the pair is configured for Jabber Guest.

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

Unsupported Endpoint Features When Using MRA

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).
- Cisco IP Phone 88xx and 78xx series support shared line or multiline features when connected through MRA (provided that Path Header support is enabled). We do not support shared line or multiline features over MRA for any other phones, endpoints, or soft clients.
- 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
- Additional mobility features including GSM handoff and session persistency.
- Hunt group/hunt pilot/hunt list.
- Self-care portal.
- Jabber SDK is not supported over MRA.

Unsupported Cisco VCS Features and Limitations When Using MRA

- The Cisco VCS cannot be used for Jabber Guest when it is used for Mobile and Remote Access (MRA).
- The Cisco VCS Control used for MRA cannot also be used for Microsoft gateway service. Microsoft gateway service 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.
- Deployments on Large VM servers are limited to 2500 proxied registrations to Unified CM (the same limit as

Cisco VCS appliances or equivalent VM).

- Not all contact center features are supported by Cisco VCS when connected through MRA.

Unsupported Contact Center Features When Using MRA

This section applies if you use the Cisco Unified Contact Center Express (Unified CCX) solution through Mobile and Remote Access (MRA).

Cisco VCS does not support some Unified CCX features for contact center agents or other users who connect over MRA. Unsupported features include:

- Deskphone control functions (due to no support for CTI-QBE protocol).
- Built in Bridge (BIB) functions, which means that silent monitoring and recording, and agent greeting are not available.
- Shared line and multiline support for 78xx and 88xx series phones is available as a preview feature from X8.9 but is not in earlier Cisco VCS versions.

Notes:

- Jabber for Mac and Jabber for Windows are not capable of deskphone control when they are connected over MRA. This is because the Cisco VCS pair does not traverse the CTI-QBE protocol.
- If these Jabber applications, or other CTI applications, can connect to CUCM CTIManager (directly or through the VPN) they *can* provide deskphone control of clients that are connected over MRA.

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 (and later).

To ensure continuous interoperability, you must upgrade your Cisco VCS systems to X8.9 *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 X8.9

Prerequisites and Software Dependencies

Upgrade Caution, PLEASE READ: X8.8 and later versions are 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 or later:

- 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.

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 or later before you upgrade IM and Presence Service to 11.5.

- Certificates: Certificate validation was 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 onward, 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 X8.9, 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

Cisco Trademark