



# Cisco TelePresence Video Communication Server X8.10.4

## Release Notes

**First Published: July 2017**

**Last Updated: September 2018**

## Preview Features Disclaimer

Some features in this release are provided in “preview” status only, because they have known limitations or incomplete software dependencies. Cisco reserves the right to disable preview features at any time without notice. Preview features should not be relied on in your production environment. Cisco Technical Support will provide limited assistance (Severity 4) to customers who want to use preview features.

## Contents

Preface .....	2
Change History .....	2
Supported Platforms .....	3
Related Documents .....	4
Feature History .....	6
Changes in X8.10.4 .....	6
Changes in X8.10.3 .....	7
Changes in X8.10.2 .....	7
Changes in X8.10.1 .....	8
Features in X8.10 .....	9
New Features for Deployments with Mobile and Remote Access .....	9
Changes to TLS and Cipher Suite Defaults .....	12
AES-GCM Cipher Mode for Media Encryption .....	13
Delayed Cisco XCP Router Restart for Multitenancy .....	14
Server Name Indication for Multitenancy .....	14
Session Identifier Support .....	15
REST API Expansion .....	15
(Preview) Smart Call Home .....	15
Other Software Changes and Enhancements .....	15

## Preface

User Interface Menu Changes .....	17
Documentation Changes .....	17
Open and Resolved Issues .....	18
Bug Search Tool Links .....	18
Notable Issues in this Version .....	18
Limitations .....	20
Some Cisco VCS Features are Preview or Have External Dependencies .....	20
Unsupported Functionality .....	20
Virtual Systems .....	20
Language Packs .....	20
Option Keys Only Take Effect for 65 Keys or Fewer .....	21
MS Lync / Office 365 Calls Fail if a Cisco VCS Expressway Cluster Node is Placed in Maintenance Mode .....	21
MS Federation with Dual Homed Conferencing .....	21
OAuth Token Authorization (Jabber) .....	21
Mobile and Remote Access .....	21
Interoperability .....	21
Notable Interoperability Concerns .....	21
Which Cisco VCS Services Can Run Together? .....	22
Upgrading to X8.10.4 .....	23
Prerequisites and Software Dependencies .....	23
Upgrade Instructions .....	25
Using Collaboration Solutions Analyzer .....	32
Using the Bug Search Tool .....	32
Obtaining Documentation and Submitting a Service Request .....	32
Cisco Legal Information .....	34
Cisco Trademark .....	34

## Preface

## Change History

**Table 1 Release Notes Change History**

Date	Change	Reason
September 2018	Update <a href="#">Limitations</a> that Cisco VCS does not support the IM and Presence Service subgroups feature over MRA connections.	Documentation
July 2018	Add caution not to use the built in Cisco VCS forward proxy.	Documentation
April 2018	Fix incorrect port information for forward proxy in <a href="#">Changes to TLS and Cipher Suite Defaults</a>	Documentation
February 2018	Update <a href="#">Limitations</a> that interoperated Microsoft calls fail if clustered Cisco VCS Expressway node placed in maintenance mode	Documentation
December 2017	Update <a href="#">Feature History</a> , <a href="#">Open and Resolved Issues</a>	X8.10.4 maintenance release

## Preface

**Table 1 Release Notes Change History (continued)**

Date	Change	Reason
November 2017	Update <a href="#">Feature History</a> , <a href="#">Open and Resolved Issues</a> and <a href="#">Limitations</a>	X8.10.3 maintenance release
October 2017	Added preview feature "Built-in-Bridge Recording over MRA"	New in X8.10.2
September 2017	Update <a href="#">Limitations</a> with maximum of 65 option keys	Documentation
September 2017	Update <a href="#">Open and Resolved Issues</a> and <a href="#">Limitations</a>	X8.10.2 maintenance release
August 2017	Clarify information about <a href="#">TURN on port 443</a>	Documentation
August 2017	Add summary of X8.10.1 software enhancements. Update <a href="#">Open and Resolved Issues</a>	X8.10.1 maintenance release
July 2017	Update <a href="#">Prerequisites and Software Dependencies</a> with information for deployments that interoperate with Microsoft environments	Documentation
July 2017	First publication	X8.10

## 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 26<sup>th</sup> 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#####.

**Advance Notice - Support for CE500 and CE1000 Appliances to be Withdrawn**

Cisco will withdraw support for the Cisco VCS CE500 and CE1000 appliance hardware platforms in a future release. More details are available in the [End-of-sale announcement](#).

## Related Documents

**Table 3 Links to Cisco VCS User Documents**

Installation	<p><b>For Expressway:</b></p> <ul style="list-style-type: none"> <li>■ <i>Cisco Expressway Virtual Machine Installation Guide</i> on the <a href="#">Expressway installation guides page</a>.</li> <li>■ <i>Cisco Expressway CE1100 Appliance Installation Guide</i> on the <a href="#">Expressway installation guides page</a>.</li> </ul> <p><b>For VCS:</b> <i>Cisco Video Communication Server CE1100 Appliance Installation Guide</i> on the <a href="#">VCS installation guides page</a>.</p>
Administration and maintenance (includes reference information)	<p><b>For Expressway:</b> <i>Cisco Expressway Administrator Guide</i> on the <a href="#">Cisco Expressway Series maintain and operate guides page</a>.</p> <p><b>For VCS:</b> <i>Cisco TelePresence VCS Administrator Guide</i> on the <a href="#">Cisco TelePresence VCS maintain and operate guides page</a>.</p> <p><b>For Expressway:</b> <i>Cisco Expressway Serviceability Guide</i> on the <a href="#">Cisco Expressway Series maintain and operate guides page</a>.</p> <p><b>For VCS:</b> <i>Cisco TelePresence VCS Serviceability Guide</i> on the <a href="#">Cisco TelePresence VCS maintain and operate guides page</a>.</p>
Registrar/ basic call control	<p><b>For Expressway:</b> <i>Cisco Expressway Registrar Deployment Guide</i> on the <a href="#">Expressway configuration guides page</a>.</p> <p><b>For VCS:</b> <i>Cisco Single VCS Control - Basic Configuration Deployment Guide</i> on the <a href="#">VCS configuration guides page</a>.</p>
Firewall traversal	<p><b>For Expressway:</b> <i>Cisco Expressway-E and Expressway-C Basic Configuration Deployment Guide</i> on the <a href="#">Expressway configuration guides page</a>.</p> <p><b>For VCS:</b> <i>Cisco TelePresence VCS Basic Configuration (Control with Expressway) Deployment Guide</i> on the <a href="#">VCS configuration guides page</a>.</p>
Cisco Spark	<a href="#">Hybrid services knowledge base</a>
Clustering	<i>Cisco Expressway Cluster Creation and Maintenance Deployment Guide</i> on the <a href="#">Cisco Expressway Series configuration guides page</a> .
Certificates	<i>Cisco Expressway Certificate Creation and Use Deployment Guide</i> on the <a href="#">Expressway configuration guides page</a> .
Unified Communications	<i>Mobile and Remote Access Through Cisco Expressway</i> on the <a href="#">Expressway configuration guides page</a> .
Cisco Meeting Server	<p><i>Cisco Expressway Options with Cisco Meeting Server and/or Microsoft Infrastructure</i> on the <a href="#">Expressway configuration guides page</a>.</p> <p><i>Cisco Meeting Server API Reference Guide</i> on the <a href="#">Cisco Meeting Server programming guides page</a>.</p> <p>Other Cisco Meeting Server configuration guides are available on the <a href="#">Cisco Meeting Server configuration guides page</a>.</p>

**Table 3 Links to Cisco VCS User Documents (continued)**

Microsoft infrastructure	<i>Cisco Expressway with Microsoft Infrastructure Deployment Guide</i> on the <a href="#">Expressway configuration guides page</a> .  <i>Cisco Jabber and Microsoft Skype for Business Infrastructure Configuration Cheatsheet</i> on the <a href="#">Expressway configuration guides page</a> .
Rest API	<i>Cisco Expressway REST API Reference Guide</i> on the <a href="#">Expressway installation guides page</a> .

## Feature History

**Table 4 Feature History by Release Number**

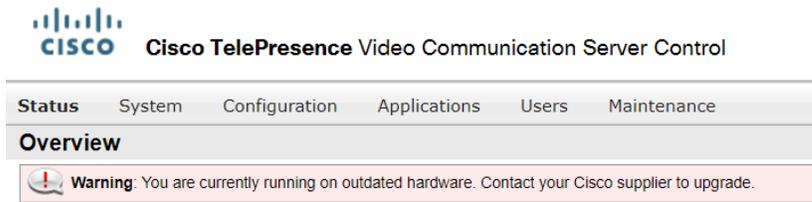
Feature / change	X8.10	X8.10.1	X8.10.2	X8.10.3 (no change)	X8.10.4 (no change)
Built-in-Bridge Recording over MRA	Not supported	Not supported	Preview	Preview	Preview
Improved Push Notification Support for MRA	Preview	Supported	Supported	Supported	Supported
Self-Describing Tokens Support for MRA (OAuth tokens with refresh)	Preview	Supported	Supported	Supported	Supported
Access Control Configuration Changes for MRA	Supported	Supported	Supported	Supported	Supported
Access Policy Support for MRA	Preview	Preview	Preview	Preview	Preview
Changes to TLS and Cipher Suite Defaults	Supported	Supported	Supported	Supported	Supported
AES-GCM Cipher Mode for Media Encryption	Supported	Supported	Supported	Supported	Supported
Delayed Cisco XCP Router Restart for Multitenancy	Supported	Supported	Supported	Supported	Supported
Server Name Indication for Multitenancy	Supported	Supported	Supported	Supported	Supported
Session Identifier Support	Supported	Supported	Supported	Supported	Supported
REST API Expansion	Supported	Supported	Supported	Supported	Supported
Smart Call Home (Not new in X8.10. Included for information due to its preview status)	Preview	Preview	Preview	Preview	Preview
Multiple Presence Domains through MRA (Not new in X8.10. Included for information due to its preview status)	Preview	Preview	Preview	Preview	Preview

## Changes in X8.10.4

- Various security enhancements to the Cisco VCS software.
- [CSCvg15240](#). Applies to deployments with IM and Presence Service federation, where the federation server is behind a NAT. Previous releases had an issue with missing presence status for a Jabber user added into a Skype for Business buddy list. The issue is now fixed.
- Clustered systems. The maximum supported round-trip delay / RTT has been tested and verified at 80ms (up from the previous verified figure of 30ms).

## Changes in X8.10.3

- The system warns you if you are on hardware that is no longer supported. Contact your Cisco supplier to find out about our migration program.



- [CSCvd68778](#) is resolved in this release, which means that Extension Mobility works via MRA for those Cisco IP Phone 7800 Series and Cisco IP Phone 8800 Series phones that support MRA.

## Changes in X8.10.3

**Important!** All Cisco VCS software versions from X8.9 include a fix for an issue with the Call History table. In certain circumstances this issue may cause severe system problems (CDETS [CSCvc58081](#) refers). If you are not already running a fixed version, then we strongly recommend that you upgrade to this X8.10.n release.

- Cisco Spark Hybrid Services. For new registrations of Cisco VCSs to Cisco Spark, the Cisco VCS must be running X8.10.3 or later. Existing registrations still work with Cisco VCS X8.9 or later, although we recommend that you always keep the host Cisco VCS at the latest feature release.
- [CSCvg09088](#). Applies to Mobile and Remote Access deployments with multiple IM and Presence Service clusters that are not all configured with the same OAuth capabilities. Previously, the Cisco VCS Control XCP component did not always communicate with a user's home IM and Presence Service cluster. This could result in a mismatch of authorization support and cause Jabber client sign-ins to fail over MRA. The issue is now fixed.
- Added a SIP maximum message size setting. A new **SIP max size** setting in the Cisco VCS user interface (**Configuration > Protocols > SIP > Advanced**) defines the maximum SIP message buffer on the Cisco VCS. The default is 32,768 bytes, and the value is configurable up to 1 MB.
- [CSCvf85709](#). From X8.10.2, dual-homed conferencing through Expressway and Meeting Server with an AVMCU invoked on the Microsoft side was limited to conferences with 10 or fewer participants. This limitation no longer exists from X8.10.3, providing the SIP maximum message size is set to 32,768 bytes or greater (see previous point).
- Removed the maximum SDP payload setting. The **SDP max size** setting is removed from the Cisco VCS user interface (it used to be on **Configuration > Protocols > SIP > Advanced**). Now replaced by the new **SIP max size**.
- This release provides new Cisco VCS language packs which reflect security changes since the previous packs were created, and the latest web user interface. Instructions for installing or updating the packs are in the *Cisco VCS Administrator Guide*. The previous language packs do not work with this release.

## Changes in X8.10.2

## (Preview) Built-in-Bridge Recording over MRA

The Cisco VCS supports Built-in-Bridge recording over MRA. This feature can help your organization to prepare for the telephone recording requirements of the European Union's *Markets in Financial Instruments Directive* (MiFID II), which comes into effect in January 2018.

When Built-in-Bridge (BiB) is enabled, Cisco Unified Communications Manager forks the call to/from the endpoint to a media recording server. BiB can be used to record calls that are made or received by users working off-premises.

BiB over MRA requires the following components:

## Changes in X8.10.1

- Any compatible clients:
  - Cisco Jabber for Windows 11.9
  - Cisco Jabber for Mac 11.9
  - Cisco Jabber for iPhone and iPad 11.9
  - Cisco Jabber for Android 11.9
  - Cisco IP Phone 7811, 7821, 7841, and 7861
  - Cisco IP Phone 8811, 8841, 8845, 8851, 8861, and 8865
- Registrar/call control agent: **Cisco Unified Communications Manager 11.5(1)SU3** (BiB is not supported on Expressway-registered endpoints)
- Edge traversal: **Cisco VCS X8.10.2**
- Recording server: Out of scope for this document.

## Other changes

- CSCvf50910 **XMPP Federation fails for multiple Cisco VCS clusters**. This was previously highlighted in the *Notable Issues* section of these release notes, and is now fixed.
- CSCve41422 **MS Interop dual-homing feature fails through Cisco VCS and Meeting Server**. This is now fixed to support up to **10 users**, providing the **SIP max size** value defined in your SIP settings is 32,768 bytes (the default) or greater.
- Various corrections to the user documentation.

**Note:** As well as these Cisco VCS changes, you no longer need to use TLSv1.0 for calls to Webex via Cisco VCS.

## Changes in X8.10.1

- The Cisco VCS Expressway TURN server can now optionally be configured on port 443 for use as a generic server - but is NOT currently supported for use with Cisco Meeting Server.  
We've done this so that clients can use TURN even in environments with restrictive firewall policies.  
Some limitations exist if you want to use port 443 for TURN:
  - Not currently supported with Cisco Meeting Server.
  - You must first change the web administrator port to a different port (**System > Administration**).
  - The option to use port 443 does not apply to large systems - Cisco VCS Expressway Large OVAs or large scale appliances.
- Cisco VCS virtual machines can now run on VMware ESXi 6.5.
- A new web interface control for the AES GCM media encryption mode is available for Mobile and Remote Access (MRA) deployments. When you add a Unified CM node (**Configuration > Unified Communications > Unified CM servers**) you can now set **AES GCM support** to *On*.
- In multitenant mode, the system hostname you configure on the **System > DNS** page of the Cisco Expressway-E and in DNS for Cisco Jabber clients to register for MRA is now case insensitive.
- These features for MRA deployments are now fully supported; previously they were in preview status:
  - Improved push notification support for Cisco Jabber users with iOS devices
  - Self-describing token authorization (OAuth tokens with refresh)

**Note:** The TURN on port 443 change was actually made in X8.10, but because it wasn't included in earlier versions of X8.10 Release Notes, for convenience it's also referenced here.

## Features in X8.10

### New Features for Deployments with Mobile and Remote Access

These changes are relevant if your Cisco VCS is configured for MRA.

#### Improved Push Notification Support for MRA

We introduced this feature in X8.10 **in preview status only**. It's fully supported from **X8.10.1**.

This feature applies if you have Cisco Jabber users with iOS devices (Cisco Jabber for iPhone and iPad) who sign in remotely. Cisco VCS deployments that are configured for MRA can support Apple's cloud-based Push Notification service. From X8.9.1, we supported Push Notifications for IM and Presence Service instant messages. From X8.10, we support them for voice and video calls too. Push Notifications are only used for Jabber for iPhone and iPad clients. Android, Windows, and Mac users are unaffected.

**Note:** If Unified CM detects a remote or mobile Jabber for iPhone and iPad connection, it always sends a Push Notification as well as a SIP Invite.

#### Prerequisites and recommendations

No specific configuration is needed on the Cisco VCS for Push Notifications, assuming Cisco VCS Expressway is already providing Mobile and Remote Access (MRA) for Jabber iOS devices. However, these prerequisites and recommendations apply:

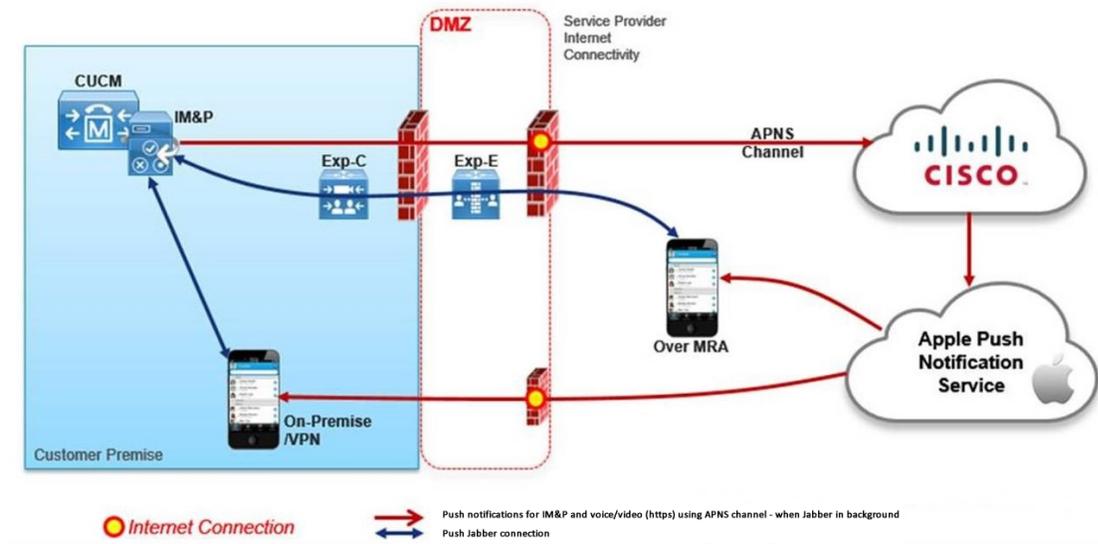
- Push Notifications in the Cisco VCS require a network connection between Cisco VCS and the Cisco WebEx cloud, and between Cisco Jabber and the Push Notification servers in the Apple cloud. **They cannot work in a private network, with no internet connection.**
- Cisco VCS is already providing Mobile and Remote Access for Jabber for iPhone and iPad. MRA must be fully configured (domain, zone, server settings).
- Depending on your Unified CM configuration, the Unified CM may need a forward proxy to send Push Notifications to the Cisco Collaboration Cloud.
- We recommend using self-describing token authorization.
- Cisco VCS Expressway **restart required for Push Notifications with instant messages**. After you enable Push Notifications on the IM and Presence Service you need to restart the Cisco VCS Expressway. Until the restart, Cisco VCS Expressway can't recognize the push capability on IM and Presence Service, and does not send PUSH messages to the Jabber clients.
- You need the following Push Notification-enabled releases (or higher) on Cisco Unified Communications Manager, IM and Presence Service, and the Jabber devices:
  - – Cisco VCS X8.10.1 or later (preview status only in X8.10)
  - – Cisco Jabber for iPhone and iPad iOS 11.9
  - – Cisco Unified Communications Manager 11.5(SU3)
  - – Cisco Unified Communications Manager IM and Presence Service 11.5(SU3)
  - – Cisco Unity Connection 11.5(SU3)

#### Why have we implemented support for Push Notifications?

Apple now deprecates the VoIP Background Mode that allows Jabber iOS to keep a SIP session open even when the app is running in the background. Push Notifications allow Unified CM to tell Jabber about incoming calls and messages. Then Jabber can reconnect to Unified CM to retrieve the message or answer the call. Jabber uses the new self-describing token feature in this release to help it to do this quickly.

## Features in X8.10

Figure 1 Push Notifications architecture



### Information about Push Notifications in Unified Communications products

For information about Push Notifications in Unified CM and IM and Presence Service, see *Deploying Push Notifications for Cisco Jabber on iPhone and iPad* available from the [Cisco Unified Communications Manager documentation pages](#) on Cisco.com.

### About the Cisco VCS forward proxy service

**CAUTION:** At present the built-in Cisco VCS forward proxy is not suitable for use with Cisco Unified Communications Manager and/or IM and Presence Service, and is not supported for those products. The forward proxy is in the Cisco VCS user interface, but it should not be used. This means that if you require a forward proxy deployment, you need to use a suitable third-party HTTPS proxy.

## Self-Describing Tokens Support for MRA (OAuth tokens with refresh)

We introduced this feature in X8.10 **in preview status only**. It's fully supported from **X8.10.1**.

Cisco VCS supports using self-describing tokens as an MRA authorization option. (Set "**Authorize by OAuth token with refresh**" to Yes.) Self-describing tokens offer significant benefits:

- Token refresh capability, so users don't have to repeatedly re-authenticate.
- Fast authorization.
- Access policy support. The Cisco VCS can enforce MRA access policy settings applied to users on the Unified CM.
- Roaming support. Tokens are valid on-premises and remotely, so roaming users don't need to re-authenticate if they move between on-premises and off-premises.

The Cisco VCS uses self-describing tokens in particular to facilitate Cisco Jabber users. Jabber users who are mobile or work remotely, can authenticate while away from the local network (off-premises). If they originally authenticate on the premises, they don't have to re-authenticate if they later move off-premises. Similarly, users don't have to re-authenticate if they move on-premises after authenticating off-premises. Either case is subject to any configured access token or refresh token limits, which may force re-authentication.

For users with Jabber iOS devices, the high speeds supported by self-describing tokens optimize Cisco VCS support for Apple Push Notifications (APNs).

## Features in X8.10

We recommend self-describing token authorization for all deployments, assuming the necessary infrastructure exists to support it. Subject to proper Cisco VCS configuration, if the Jabber client presents a self-describing token then the Cisco VCS simply checks the token. No password or certificate-based authentication is needed. The token is issued by Unified CM (regardless of whether the configured authentication path is by external IdP or by the Unified CM). Self-describing token authorization is used automatically if all devices in the call flow are configured for it.

The Cisco VCS Control performs token authorization. This avoids authentication and authorization settings being exposed on Cisco VCS Expressway.

**Prerequisites**

- Cisco VCS is already providing Mobile and Remote Access for Cisco Jabber.
- All other devices in the call flow are similarly enabled.
- You have the following minimum product versions installed, or later:
  - Cisco VCS X8.10.1 (preview status only in X8.10)
  - Cisco Jabber 11.9 (on any/all client platforms)  
If you have a mix of Jabber devices, with some on an older software version, the older ones will use simple OAuth token authorization (assuming SSO and an IdP are in place).
  - Cisco Unified Communications Manager 11.5(SU3)
  - Cisco Unified Communications Manager IM and Presence Service 11.5(SU3)
  - Cisco Unity Connection 11.5(SU3)
- Make sure that self-describing authentication is enabled on the Cisco Expressway-C ("**Authorize by OAuth token with refresh**" setting) and on Unified CM and/or IM and Presence Service ("**OAuth with Refresh Login Flow**" enterprise parameter).
- You must refresh the Unified CM nodes defined on the Cisco VCS. This fetches keys from the Unified CM that the Cisco VCS needs to decrypt the tokens.

**Limitations**

**Important:** From X8.10.1, the Cisco VCS fully supports the benefits of self-describing tokens (including token refresh, fast authorization, and access policy support). However, not all of the benefits are actually available throughout the wider solution. Depending on what other products you use (Unified CM, IM and Presence Service, Cisco Unity Connection) and what versions they are on, not all products fully support all benefits of self-describing tokens.

**Note about automated intrusion protection**

With OAuth token authentication, in some circumstances Cisco Jabber may trigger the automated intrusion protection on the Cisco VCS Expressway. If this happens, a workaround is described in the Troubleshooting appendix of the *Mobile and Remote Access Via Cisco VCS Deployment Guide* on [Cisco VCS configuration guides page](#).

## Access Control Configuration Changes for MRA

Configuration for MRA access control (authentication and authorization settings) is improved in this release.

- You can configure a more detailed, granular level of control than before.
- All configuration settings are collected onto the Cisco VCS Control.
- Single sign-on authorization in previous releases is now simple OAuth token authorization. The web UI option is **Authorize by OAuth token**.
- The setting **Check for internal SSO availability** in previous releases is now **Check for internal authentication availability**.
- MRA access control previously defaulted to username and password authorization, which did not need explicit configuration. From X8.10, if you want username and password authorization you must manually configure it. The web UI option is **Authorize by user credentials**.

## Features in X8.10

- For new customers, the MRA access control settings default to self-described token authorization, managed by the Unified CM (not an external IdP), with all other access control options off.
- Although you still enable MRA itself on Cisco VCS Expressway, the MRA access control settings are now configured on Cisco VCS Control.

**Important: Information for existing MRA customers**

If you already use the Cisco VCS with MRA, the upgrade cannot preserve all of your existing settings. The X8.10 software **overwrites your currently configured MRA access control values**. The new upgrade values are detailed in the [upgrade instructions](#) later in these notes.

Because of these changes, we recommend some additional pre-upgrade checks and post-upgrade configuration for this release. The necessary steps are also described later in the upgrade instructions.

**(Preview) Access Policy Support for MRA**

This feature is currently in preview status only.

From X8.10, the Cisco VCS will enforce MRA access policy settings specified on the Unified CM. These are optionally configured on the user profiles in Unified CM, to define which services individual users can access (None, IM&P, Voice & Video, or All). The Cisco VCS only enforces MRA access policy if these conditions apply:

- The Cisco VCS is configured to process self-describing tokens for MRA authorization (set **Authorize by OAuth token with refresh** to *On*).
- Other products in the call path also support self-describing tokens, including the access policy element of the tokens.

**Note:** As MRA access policy can only be enforced if the clients use self-describing tokens, it's most effective when self-describing token authorization is the *only* permitted authorization method for MRA.

**Changes to TLS and Cipher Suite Defaults**

From X8.10, VCS defaults to TLS version 1.2 when establishing secure connections for the following services:

- HTTPS
- SIP
- XMPP
- UC server discovery
- Forward proxy
- Reverse proxy

For improved security, TLS 1.2 is recommended for all encrypted sessions. If required (typically for compatibility reasons with legacy equipment) the minimum TLS versions can be configured to use versions 1.0 or 1.1.

On upgrade, previous behavior and defaults persist so you won't be defaulted to TLS version 1.2. However, new installations will use the new defaults. So for new installations you should check that TLS version 1.2 is supported by all browsers and equipment that must connect to VCS.

**New cipher suites from X8.10**

You can configure the cipher suite and minimum supported TLS version for each service on the new **Maintenance > Security > Ciphers** page, and they are also configurable via the CLI and the API. More information is provided in the online help and *Administrator Guide*.

These services and new cipher suites are shown in the table (cipher strings are in OpenSSL format):

## Features in X8.10

Services	Cipher Suite Values (Defaults)
Forward proxy TLS ciphers	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL
HTTPS ciphers	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL
Reverse proxy TLS ciphers	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL
SIP TLS ciphers	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:+ADH
UC server discovery TLS ciphers	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL
XMPP TLS ciphers	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL

**CLI cipher suite changes from X8.10**

The cipher configuration changed from `xConfig Sip TLS CipherSuites` to `xConfig Ciphers SIPTLSCiphers` value. This uses the same format as the new configuration for ciphers for the other services.

The maximum string length for cipher suites is now 2048 characters.

**Known issues with TLS version 1.2 support**

- Legacy endpoint version support:
  - MXP and TE Series devices do not support TLSv1.2.
  - TC < 7.3.3 does not support TLSv1.1 or TLSv1.2.
  - TC 7.3.6 removed support for TLSv1.0.
  - Jabber Video for TelePresence on Windows 7 does not support TLSv1.1/1.2 (supported from Windows 8.1).
- Windows:
  - Windows 7 and Windows Server 2008 R2 added TLSv1.1/1.2 support but **off** by default; post Windows 8.1 they are on by default. This impacts Jabber Video for TelePresence, TMS, Lync and other software and services running on Windows using the OS TLS APIs.
  - Windows OS 2003 does not support TLSv1.1 or TLSv1.2.
- Third-party endpoints:
  - Lifesize Icon 600 does not support TLSv1.2.
- Restarts:
  - SIP requires a restart after changing cipher suite configuration or TLS protocol version.
  - XCP requires a restart after changing cipher suite configuration or TLS protocol version.

**Ports**

The forward proxy destination port is 8445 and the source port is ephemeral. (The Expressway forward proxy is dependent on support by your Unified CM software.)

The reverse proxy listens on port 8443.

## AES-GCM Cipher Mode for Media Encryption

As part of our ongoing security improvement work, from X8.10 we've improved the media encryption capabilities of the Cisco VCS. All zones that can do media encryption now support the AES-GCM cipher mode for encrypting / decrypting SRTP media streams. (AES-GCM refers to the Galois/Counter Mode used with Advanced Encryption Standard cipher.)

## Features in X8.10

This feature is off by default. If you know your endpoints can use GCM to encrypt media, then you may see a performance improvement by enabling this mode on the zones in the media path.

**Notes:**

- As the new media encryption mode is off by default, it is off for the CETls zones that are automatically created for MRA. These zones are not editable through the web interface. To use AES GCM media encryption with MRA:
  - Zones that have not yet been auto-created. When you add the Unified CM server (**Configuration > Unified Communications > Unified CM servers**) set **AES GCM support** to *On*. (This web UI setting was introduced in X8.10.1.)
  - Zones that already exist. Configure the zones using the CLI command `xConfiguration Zones Zone index Neighbor SIP Media AesGcm Support: "On"` (Use `xstatus zone` to list the zones and their index numbers.)
- CE Series endpoints, and 7800 Series and 8800 Series phones don't know that they can offer AES GCM media encryption when they are in "edge" mode. They can offer this media encryption when they are directly registered to Unified CM (not through MRA).  
When these endpoints register through MRA, the Cisco VCS Control will negotiate AES-128 media encryption with them instead.
- Cisco Jabber 11.9 can negotiate AES GCM, but it is not enabled by default when Jabber is in "edge" mode. You can modify the behavior using the *EnableNGEPolicy* parameter. See the *Parameters Reference Guide for Cisco Jabber* at the [Jabber install and upgrade guides page](#).

## Delayed Cisco XCP Router Restart for Multitenancy

The delayed Cisco XCP Router restart feature is part of Cisco Hosted Collaboration Solution (HCS), and is only available when the Cisco VCS Expressway is in multitenant mode. The Cisco VCS Expressway enters multitenant mode when you add a second Unified CM traversal zone with a new SIP domain.

**Note:** In multitenant mode, you must configure the system hostname on the **System > DNS** page of the Cisco Expressway-E to match the hostname configured in DNS (case-specific before X8.10.1, case insensitive from X8.10.1). Otherwise Cisco Jabber clients will be unable to register successfully for MRA.

Multitenancy allows a service provider to share an Cisco VCS Expressway cluster among multiple tenants. Each tenant has a dedicated Cisco VCS Control cluster that connects to the shared Cisco VCS Expressway cluster.

Certain configuration changes on the Cisco VCS Expressway cluster, or a customer's Cisco VCS Control cluster, require a restart of the Cisco XCP Router on each Cisco VCS Expressway in the shared cluster. The restart is required for Cisco XCP Router configuration changes to take effect across all nodes in a multitenant Cisco VCS Expressway cluster. The restart affects all users across all customers.

To reduce the frequency of this restart, and the impact on users, you can use the delayed Cisco XCP Router restart feature.

**Note:** Without the delayed restart feature enabled, the restart happens automatically and occurs each time you save any configuration change that affects the Cisco XCP Router. If multiple configuration changes are required, resulting in several restarts of the Cisco XCP Router, it can adversely affect users. We strongly recommend that multitenant customers enable the delayed Cisco XCP Router restart feature.

## Server Name Indication for Multitenancy

Multitenancy is part of Cisco Hosted Collaboration Solution (HCS), and allows a service provider to share a Cisco VCS Expressway cluster among multiple tenants.

Using the Server Name Indication (SNI) protocol extension within TLS, the Cisco VCS can now store and use domain-specific certificates that can be offered to a client during the TLS handshake. This capability allows seamless integration of endpoints registering through MRA in a multitenant environment, and ensures the certificate domain name matches the client's domain. During a TLS handshake, the client includes an SNI field in the *ClientHello*

## Features in X8.10

request. The Cisco VCS looks up its certificate store and tries to find a match for the SNI hostname. If a match is found the domain-specific certificate is returned to the client.

**Note:** In multitenant mode, you must configure the system hostname on the **System > DNS** page of the Cisco Expressway-E to match the hostname configured in DNS (case-specific before X8.10.1, case insensitive from X8.10.1). Otherwise Cisco Jabber clients will be unable to register successfully for MRA.

See *Multitenancy with Cisco Expressway* on the [Cisco Hosted Collaboration Solution page](#).

## Session Identifier Support

From X8.10 the Cisco VCS can support SIP "session identifiers". Assuming all devices in the call use session identifiers, the mechanism uses the *Session-ID* field in SIP headers to maintain a unique code through the entire transit of a call. Session identifiers are useful for investigating issues with calls that involve multiple components, as they can be used to find and track a specific call on the Cisco VCS server. Support for session identifiers includes the SIP side of interworked SIP/H.323 calls, and calls to and from Microsoft systems. Session identifiers are defined in [RFC 7989](#).

## REST API Expansion

In X8.10, the API to simplify remote configuration has been expanded. Third party systems, such as Cisco Prime Collaboration Provisioning, can now use the API to configure the following features / services on the Cisco VCS:

- Admin account
- Firewall rules
- SIP configuration
- TURN server configuration
- Domain certificates for Server Name Identification

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](#).

## (Preview) Smart Call Home

This feature is currently in preview status only.

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.

## Other Software Changes and Enhancements

- The upgrade process between major releases (for example, from X7.*n* to X8.*n*) has always needed a release key. The upgrade process now makes it clearer to administrators when a key is needed. And provides an opportunity to enter the key after you start the upgrade.

## Features in X8.10

- You can now specify that anyone signing in to the Cisco VCS must first acknowledge a customizable welcome message. The system displays an acceptance button, which users must click before they're allowed to continue.
- From X8.10, the Certificate Signing Request (CSR) generator no longer allows you to select the SHA-1 Digest algorithm for your certificate's signature. The remaining options are SHA-256, SHA-384, and SHA-512.
- The upload mechanism for server security certificates (**Maintenance > Security > Server certificate**) displays a warning if the certificate fails to meet certain criteria. Cases when the warning is displayed include:
  - Certificate does not have an acceptable level of security.
  - Certificate is missing a common name (CN) attribute.

An alarm is also raised in this case, because some Cisco VCS services don't work without the common name (MRA, Jabber Guest, and the Web Proxy for Cisco Meeting Server).
  - The certification authority (CA) or certificate revocation list (CRL) is not recognized.The certificate upload is not prevented.
- For devices connected through MRA, the Cisco VCS now provides passthrough support of Unified CM shared line features on Cisco Jabber clients running 11.9 or later, and on Collaboration Endpoint devices running CE8.3.0 or later. (The previous Cisco VCS release already supported shared line for MRA-connected Cisco IP Phone 78xx and 8811, 8841, 8845, 8861 and 8865 devices with Path Header support enabled.)
- The Cisco VCS Expressway TURN server can now optionally be configured on port 443 for use as a generic server - but is NOT currently supported for use with Cisco Meeting Server.

We've done this so that clients can use TURN even in environments with restrictive firewall policies. Some limitations exist if you want to use port 443 for TURN:

  - Not currently supported with Cisco Meeting Server.
  - You must first change the web administrator port to a different port (**System > Administration**).
  - The option to use port 443 does not apply to large systems - Cisco VCS Expressway Large OVAs or large scale appliances.
- From X8.10, the requirement to have a 10 Gbps NIC in order to achieve the scalability of a large system is removed. It is now possible to have the capacity of a large system with a 1 Gbps NIC subject to your bandwidth constraints.

However, if you upgrade a Medium system with a 1 Gbps NIC to X8.10 or later, Cisco VCS automatically converts the system to a Large system. As a result, Cisco VCS Expressway listens for multiplexed RTP/RTCP traffic on default demultiplexing ports for Large systems (36000 to 36011); instead on demultiplexing ports that are configured for Medium systems. In this case, the Cisco VCS Expressway drops the calls because these ports (36000 to 36011) are not open on the firewall. If you encounter this problem, open the default demultiplexing ports for Large systems on the firewall.
- Cisco VCS **no longer supports ESXi 5.0 or ESXi 5.1 for virtual deployments**. You must use ESXi 5.5 or ESXi 6.0 (or ESXi6.5 if you have Cisco VCS X8.10.1). See <https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/product-lifecycle-matrix.pdf>
- The IX filtering setting (**SIP UDP/IX filter mode**) defaults to *Off* for the preconfigured **Cisco Unified Communications Manager** zone profile. Previously the default was *On*. The default is still *On* for other preconfigured profiles, including **Cisco Unified Communications Manager (8.6.1 or later)**.

## User Interface Menu Changes

- Hybrid Services changes:
  - From version X8.10, the connectors used for some Cisco Spark Hybrid Services may co-reside with the Cisco VCS Control that is used with Call Service. This co-residency is subject to limitations on user numbers as described in the relevant Hybrid Services documentation. Previously we recommended a dedicated Cisco VCS Control for hosting the connectors. See [Hybrid Services documentation](#) for more detail.
  - Cisco VCSs that will be used to host connectors for Cisco Spark Hybrid Services, must be on version X8.10.3 or later before you register them to Cisco Spark.

If the connector host Cisco VCS is already registered to Cisco Spark then we still support X8.9. However, to maintain compatibility we recommend that you keep the host Cisco VCS up to date with the latest feature release. The Cisco VCS-based connectors check the host version and warn if it's more than one feature release behind. For example, when X8.10 is the latest feature release, the connectors will work with X8.9 and X8.10. We cannot guarantee compatibility with older versions of the host Cisco VCS.

## User Interface Menu Changes

Some menu names in the Web UI are different in this release, as follows:

- **Maintenance > Security Certificates** is now just **Maintenance > Security**
- **Status > Unified Communications > SSO Statistics** is now **Status > Unified Communications > MRA Authentication Statistics**
- **HTTP allow list > Editable rules** is now **HTTP allow list > Editable inbound rules**
- **HTTP allow list > Automatically added rules** is now **HTTP allow list > Automatic inbound rules**
- **HTTP allow list > Automatic outbound rules** is new in this release
- Various other new menus are added to support the features introduced by this release

## Documentation Changes

**We continue to phase out Cisco VCS documentation.** Previously we provided two separate variants of most customer support documents, for the VCS and the Expressway. From X8.10 we begin to provide Expressway versions only. The Expressway versions will include any relevant VCS-specific information. This change will happen gradually over time.

- Cisco Expressway documents: <http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/tsd-products-support-series-home.html>
- Cisco VCS documents: <http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/tsd-products-support-series-home.html>

**MRA limitations removed from Release Notes.** We've removed the lists of unsupported items in Mobile and Remote Access from the Limitations section of these notes. This information is available in the *Mobile and Remote Access Through Cisco Expressway Deployment Guide* on the [Expressway Configuration Guides](#) page.

**Minor enhancements to the documents.** As well as adding the release features, we've made some minor documentation corrections and changes.

## Open and Resolved Issues

### Bug Search Tool Links

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 X8.10.4](#)
- [Issues resolved by X8.10.3](#)
- [Issues resolved by X8.10.2](#)
- [Issues resolved by X8.10.1](#)
- [Issues resolved by X8.10](#)

### Notable Issues in this Version

#### **Rich Media Session license is not consumed by Single NIC Cisco VCS Expressway hosting Jabber Guest service** [CSCva36208](#)

Changes to the licensing model in X8.8 revealed an issue with licensing of the Jabber Guest service on the Cisco VCS Expressway server. When the Cisco VCS pair is part of the "Single NIC" Jabber Guest deployment, the Cisco VCS Expressway should count one RMS license for each Jabber Guest call, but it does not. This issue may cause confusion about the server's load, because usage appears low even when the server is processing multiple calls.

We recommend the Dual NIC Jabber Guest deployment. If you are using the single NIC deployment, make sure your Cisco VCS Expressway is correctly licensed to ensure continuity of service with future upgrades.

#### **Cisco VCS B2BUA drops some RTCP multistreaming Refresh packets during decryption in Cisco WebEx calls** [CSCvc47502](#) and [CSCvc34689](#)

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

## Open and Resolved Issues

- 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

### Some Cisco VCS Features are Preview or Have External Dependencies

**Important!** We aim to provide new Expressway features as speedily as possible. Sometimes it is not possible to officially support a new feature because it may require updates to other Cisco products which are not yet available, or known issues or limitations affect some deployments of the feature. Where customers may still benefit from using the feature, it will be marked as "preview" in the release notes. Preview features may be used, but you should not rely on them in production environments (see [Preview Features Disclaimer, page 1](#)). Occasionally, we may recommend that a feature is not used until further updates are made to Expressway or other products.

The following Cisco VCS features are currently provided in preview status only, or depend on other product software versions which are not yet available

- Built-in-Bridge Recording over MRA
- Access Policy Support for MRA
- Smart Call Home
- Multiple Presence Domains through MRA

### Unsupported Functionality

- The Cisco VCS does not terminate DTLS. We do not support DTLS for securing media. SRTP is used to secure calls instead, and attempts to make DTLS calls through Cisco VCS will fail.  
The Cisco VCS does insert the DTLS protocol in the SDP, but only for the purpose of traversing the encrypted iX protocol.
- The Cisco VCS does not support the SIP UPDATE method ([RFC 3311](#)). Features that rely on this method will not work as expected.
- 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.
- **CAUTION: At present the built-in Cisco VCS forward proxy is not suitable for use with Cisco Unified Communications Manager and/or IM and Presence Service, and is not supported for those products. The forward proxy is in the Cisco VCS user interface, but it should not be used. This means that if you require a forward proxy deployment, you need to use a suitable third-party HTTPS proxy.**

### Virtual Systems

With physical Cisco VCS appliances, the **Advanced Networking** option allows the speed and duplex mode to be set for each configured Ethernet port. You cannot set port speeds for virtual machine-based Cisco VCS systems.

Also, virtual machine-based systems always show the connection speed between Cisco VCS and Ethernet networks as 10000 Mb/s, regardless of the actual physical NIC speed. This is due to a limitation in virtual machines, which cannot retrieve the actual speed from the physical NIC(s).

### Language Packs

If you translate the Cisco VCS web user interface, new Cisco VCS language packs are available from X8.10.3. Older language packs do not work with X8.10.n software (or X8.9.n). Instructions for installing or updating the packs are in the *Cisco VCS Administrator Guide*.

## Interoperability

### Option Keys Only Take Effect for 65 Keys or Fewer

If you try to add more than 65 option keys (licenses), they appear as normal in the Cisco VCS web interface (**Maintenance > Option keys**). However, only the first 65 keys take effect. Additional keys from 66 onwards appear to be added, but actually the Cisco VCS does not process them.

CDETS [CSCvf78728](#) refers.

### MS Lync / Office 365 Calls Fail if a Cisco VCS Expressway Cluster Node is Placed in Maintenance Mode

This applies if you have clustered Cisco VCS Expressway nodes and interoperate with Microsoft environments. If you place one of the Cisco Expressway-Es in maintenance mode, Lync or Office 365 calls fail. This is because current lookup behavior by the Lync Edge server / Office 365 cloud is to fetch the FQDN of the *non-active* (maintenance mode) Cisco VCS Expressway. Hence the call requests always fail.

### MS Federation with Dual Homed Conferencing

If you use dual homed conferencing through Cisco VCS and Meeting Server with an AVMCU invoked on the Microsoft side, the maximum SIP message size must be set to 32768 bytes (the default) or greater. Defined via **SIP max size** on **Configuration > Protocols > SIP**.

### OAuth Token Authorization (Jabber)

For Jabber users, some limitations may exist with enforcing OAuth authorization by self-describing token as the only allowed authentication method. Users on older versions of Jabber can still authenticate by username and password, or traditional single sign-on.

## Mobile and Remote Access

- Feature Limitations

If you use Cisco VCS for Mobile and Remote Access (MRA), some unsupported features and limitations currently exist. These are detailed in the *Mobile and Remote Access Through Cisco VCS Deployment Guide* on the [VCS Configuration Guides](#) page. Note that the following item was added to that guide after its initial publication for X8.10.x:

In this release, Cisco VCS does not support the IM and Presence Service subgroups feature. If you use subgroups over MRA, Cisco Jabber logins will fail, or will fail intermittently.

- Endpoint Limitations

Some recent Cisco IP Phones in both the 8800 Series and 7800 Series do not currently support MRA. For details of which 7800/8800 Series phones support MRA, see the "Prerequisites" section of the latest *Mobile and Remote Access Through Cisco Expressway* guide, or ask your Cisco representative.

## 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).

## Which Cisco VCS Services Can Run Together?

To ensure continuous interoperability, you must upgrade your Cisco VCS systems to X8.10 *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>. AXI query HTTP error "'HTTPError:500'"
```

## Which Cisco VCS Services Can Run Together?

The *Cisco Expressway Administrator Guide* on the [Cisco Expressway Series maintain and operate guides](#) page details which Cisco VCS services can coexist on the same Cisco VCS system or cluster. See the table "*Services That Can be Hosted Together*" in the Introduction section. For example, if you want to know if MRA can coexist with CMR Cloud (it can) the table will tell you.

## Upgrading to X8.10.4

### Prerequisites and Software Dependencies

**CAUTION:** This section has important information about upgrade issues that may prevent the system working properly after an upgrade. Before you upgrade, please review this section and complete any tasks that apply to your deployment.

#### All Deployments

We do not support downgrades. Do not install a previous Cisco VCS version onto a system that is running a newer version. If you do so, the system configuration will not be preserved.

X8.8 and later versions are more secure than earlier versions. Upgrading could cause your deployments to stop working as expected, and you must check for the following environmental issues before you upgrade to X8.8 or later:

- Certificates: Certificate validation was tightened up in X8.8.
  - Try the secure traversal test before and after upgrade (**Maintenance > Security > 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?

From 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.

From X8.8, clustering communications 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.

- (If you use the Cisco VCS for Mobile and Remote Access) 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 Expressway* on the [Expressway 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.

#### Deployments that Use the Cisco VCS for Mobile and Remote Access

- **Cisco VCS Control and Cisco Expressway-E should be upgraded together.** We don't recommend operating with Cisco VCS Control and Cisco VCS Expressway on different versions for an extended period.

## Upgrading to X8.10.4

- X8.10.*n* moves the MRA authentication (access control) settings from Cisco VCS Expressway to Cisco VCS Control, **and applies default values where it is not possible to retain your existing settings**. For correct system operation, after you upgrade you must reconfigure the access control settings on the Cisco VCS, as described later in these upgrade instructions.

### Deployments that Use Cisco Spark Hybrid Services

The Management Connector must be up to date before you upgrade Cisco VCS. You must authorize and accept any Management Connector upgrades advertised by the Cisco Collaboration Cloud before you try to upgrade Cisco VCS. Failure to do so may cause issues with the connector after the upgrade.

For new registrations of Cisco VCSs to Cisco Spark, the Cisco VCS must be running X8.10.3 or later. Existing registrations still work with Cisco VCS X8.9 or later, although we recommend that you always keep the host Cisco VCS at the latest feature release.

### Existing Non-AES Build Installations

As of version X8.1, the software uses AES encryption. Before this a version that used weaker encryption was available. If you are upgrading 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

### Before You Begin

Make sure all relevant tasks in [Prerequisites and Software Dependencies, page 23](#) are complete.

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

#### **(If you use MRA) Note your MRA authentication settings before upgrading**

This section only applies if you use the Cisco VCS for Mobile and Remote Access and you upgrade from X8.9n or earlier to X8.10 or later. From version X8.10 we moved the MRA authentication (access control) settings from the Cisco VCS Expressway to the Cisco VCS Control. As the upgrade does not preserve the existing Cisco Expressway-E settings, after the upgrade you need to review the MRA access control settings on the Cisco VCS Control and adjust them as necessary for your deployment.

To access existing MRA authentication settings:

1. On the Cisco VCS Expressway, go to **Configuration > Unified Communications > Configuration** and locate **Single Sign-on support**. Note the existing value (On, Exclusive, or Off)
2. If **Single Sign-on support** is set to On or Exclusive, also note the current values of these related fields:
  - a. **Check for internal authentication availability**
  - b. **Allow Jabber iOS clients to use embedded Safari**

#### **(If you use MRA with clustered Unified CMs) Install latest maintenance release on TC/CE endpoints**

This section only applies if you are upgrading a Cisco VCS that is used for MRA, with clustered Unified CMs and endpoints running TC or Collaboration Endpoint (CE) software. In this case you must install the relevant TC or CE maintenance release listed below (or later) *before* you upgrade the Cisco VCS. This is required to avoid a known problem with failover. If you do not have the recommended TC/CE maintenance release, an endpoint will not attempt failover to another Unified CM if the original Unified CM to which the endpoint registered fails for some reason. CDETS [CSCvh97495](#) refers.

- TC7.3.11
- CE8.3.3
- CE9.1.2

### Process

This process does not apply if you are upgrading a Cisco VCS that uses clustering, device provisioning (Cisco TMSPE), or FindMe (with Cisco TMS managing Cisco VCS). In those cases, follow the directions in the *Cisco VCS Cluster Creation and Maintenance Deployment Guide* instead.

1. Backup the Cisco VCS system before you upgrade (**Maintenance > Backup and restore**).
2. Enable maintenance mode:
  - a. Go to **Maintenance > Maintenance mode**.
  - b. Set **Maintenance mode** to *On*.
  - c. Click **Save** and click **OK** on the confirmation dialog.
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**).

## Upgrading to X8.10.4

**4. Upgrade and restart the Cisco VCS (Maintenance > Upgrade).**

If you are upgrading to a new *major* release, for example from X7.n to X8.n, you first need to obtain a new release key from Cisco. The key is required during 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.

**5. This step depends on whether or not you use the Cisco VCS for MRA:**

- If you don't use MRA, the upgrade is now complete and all Cisco VCS configuration should be as expected.
- If you do use MRA, go on to the next section and reconfigure your MRA access control settings.

## 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.

Some services, like Mobile and Remote Access, require both the Cisco VCS Control and Cisco VCS Expressway systems to be running the same software version.

## Post-Upgrade Tasks for MRA Deployments

This section only applies if you use the Cisco VCS for Mobile and Remote Access and you upgrade from X8.9n or earlier to X8.10 or later. After the system restarts you need to reconfigure the MRA access control settings:

- 1. On the Cisco VCS Control, go to Configuration > Unified Communications > Configuration > MRA Access Control.**
- 2. Do one of the following:**
  - To take advantage of the new MRA access control methods from X8.10, set the appropriate values on this page for your chosen methods. See the first table below for help about which values to apply.
  - Or to retain your pre-upgrade authentication approach, set the appropriate values on this page to match your previous settings on the Cisco VCS Expressway. See the second table below for help about how to map the old Cisco VCS Expressway settings to their new equivalents on the Cisco VCS Control.
- 3. If you configure self-describing tokens (Authorize by OAuth token with refresh), refresh the Unified CM nodes: Go to Configuration > Unified Communications > <UC server type> and click Refresh servers.**

### Important!

- The **Check for internal authentication availability** setting will be off after the upgrade. Depending on the authentication settings on the Unified CM, this may prevent remote login by some Cisco Jabber users.
- The *Exclusive* option in X8.9 is now configured by setting **Authentication path** to *SAML SSO authentication*. This has the effect of prohibiting authentication by username and password.

The fields you actually see in the Web UI depend on whether MRA is enabled (**Unified Communications mode** set to *Mobile and remote access*) and on the selected authentication path. Not all the fields in the table are necessarily displayed.

**Table 5 Settings for MRA access control**

Field	Description	Default
Authentication path	<p>Hidden field until MRA is enabled. Defines how MRA authentication is controlled.</p> <p><i>SAML SSO authentication:</i> Clients are authenticated by an external IdP.</p> <p><i>UCM/LDAP basic authentication:</i> Clients are authenticated locally by the Unified CM against their LDAP credentials.</p> <p><i>SAML SSO and UCM/LDAP:</i> Allows either method.</p> <p><i>None:</i> No authentication is applied. The default until MRA is first enabled. The "None" option is required (rather than just leaving MRA turned off) because some deployments must turn on MRA to allow functions which are not actually MRA. (Such as the Web Proxy for Meeting Server, or XMPP Federation.) Only these customers should use "None". <b>It is not recommended in other cases.</b></p>	<p>None before MRA turned on</p> <p>UCM/LDAP after MRA turned on</p>
Authorize by OAuth token with refresh	<p>This option requires self-describing tokens for authorization. It's our recommended authorization option for all deployments that have the infrastructure to support them.</p> <p>Only Jabber clients are currently capable of using this authorization method. Other MRA endpoints do not currently support it. The clients must also be in OAuth token with refresh authorization mode.</p> <p><b>Important:</b> From X8.10.1, the Cisco VCS fully supports the benefits of self-describing tokens (including token refresh, fast authorization, and access policy support). However, not all of the benefits are actually available throughout the wider solution. Depending on what other products you use (Unified CM, IM and Presence Service, Cisco Unity Connection) and what versions they are on, not all products fully support all benefits of self-describing tokens.</p>	On
Authorize by OAuth token (previously SSO Mode)	<p>Available if <b>Authentication path</b> is <i>SAML SSO</i> or <i>SAML SSO and UCM/LDAP</i>.</p> <p>This option requires authentication through the IdP. Currently, only Jabber clients are capable of using this authorization method, which is not supported by other MRA endpoints.</p>	Off
Authorize by user credentials	<p>Available if <b>Authentication path</b> is <i>UCM/LDAP</i> or <i>SAML SSO and UCM/LDAP</i>.</p> <p>Clients attempting to perform authentication by user credentials are allowed through MRA. This includes Jabber, and supported IP phone and TelePresence devices.</p>	Off

**Table 5 Settings for MRA access control (continued)**

Field	Description	Default
Check for internal authentication availability	<p>Available if <b>Authorize by OAuth token with refresh</b> or <b>Authorize by OAuth token</b> is enabled.</p> <p>The default is No, for optimal security and to reduce network traffic.</p> <p>Controls how the Cisco VCS Expressway reacts to remote client authentication requests by selecting whether or not the Cisco VCS Control should check the home nodes.</p> <p>The request asks whether the client may try to authenticate the user by OAuth token, and includes a user identity with which the Cisco VCS Control can find the user's home cluster:</p> <p><b>Yes:</b> The <code>get_edge_sso</code> request will ask the user's home Unified CM if OAuth tokens are supported. The home Unified CM is determined from the identity sent by the Jabber client's <code>get_edge_sso</code> request.</p> <p><b>No:</b> If the Cisco VCS is configured not to look internally, the same response will be sent to all clients, depending on the Edge authentication settings.</p> <p>The option to choose depends on your implementation and security policy. If all Unified CM nodes support OAuth tokens, you can reduce response time and overall network traffic by selecting <i>No</i>. Or select <i>Yes</i> if you want clients to use either mode of getting the edge configuration - during rollout or because you can't guarantee OAuth on all nodes.</p> <p><b>Caution: Setting this to Yes has the potential to allow rogue inbound requests from unauthenticated remote clients.</b> If you specify No for this setting, the Cisco VCS prevents rogue requests.</p>	No

**Table 5 Settings for MRA access control (continued)**

Field	Description	Default
Identity providers: Create or modify IdPs	<p>Available if <b>Authentication path</b> is <i>SAML SSO</i> or <i>SAML SSO and UCM/LDAP</i>.</p> <p><b>Selecting an Identity Provider</b></p> <p>Cisco Collaboration solutions use SAML 2.0 (Security Assertion Markup Language) to enable SSO (single sign-on) for clients consuming Unified Communications services.</p> <p>If you choose SAML-based SSO for your environment, note the following:</p> <ul style="list-style-type: none"> <li>■ SAML 2.0 is not compatible with SAML 1.1 and you must select an IdP that uses the SAML 2.0 standard.</li> <li>■ SAML-based identity management is implemented in different ways by vendors in the computing and networking industry, and there are no widely accepted regulations for compliance to the SAML standards.</li> <li>■ The configuration of and policies governing your selected IdP are outside the scope of Cisco TAC (Technical Assistance Center) support. Please use your relationship and support contract with your IdP Vendor to assist in configuring the IdP properly. Cisco cannot accept responsibility for any errors, limitations, or specific configuration of the IdP.</li> </ul> <p>Although Cisco Collaboration infrastructure may prove to be compatible with other IdPs claiming SAML 2.0 compliance, only the following IdPs have been tested with Cisco Collaboration solutions:</p> <ul style="list-style-type: none"> <li>■ OpenAM 10.0.1</li> <li>■ Active Directory Federation Services 2.0 (AD FS 2.0)</li> <li>■ PingFederate® 6.10.0.4</li> </ul>	–
Identity providers: Export SAML data	<p>Available if <b>Authentication path</b> is <i>SAML SSO</i> or <i>SAML SSO and UCM/LDAP</i>.</p> <p>For details about working with SAML data, see <a href="#">SAML SSO Authentication Over the Edge, page 1</a>.</p>	–
Allow Jabber iOS clients to use embedded Safari	<p>By default the IdP or Unified CM authentication page is displayed in an embedded web browser (not the Safari browser) on iOS devices. That default browser is unable to access the iOS trust store, and so cannot use any certificates deployed to the devices.</p> <p>This setting optionally allows Jabber on iOS devices to use the native Safari browser. Because the Safari browser <i>is</i> able to access the device trust store, you can now enable password-less authentication or two-factor authentication in your OAuth deployment.</p> <p>A potential security issue exists for this option. The mechanism to return browser control from Safari to Jabber after the 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.</p> <p>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 <b>not</b> enable the embedded Safari browser.</p>	No

## Upgrading to X8.10.4

**Table 5 Settings for MRA access control (continued)**

Field	Description	Default
SIP token extra time to live	Available if <b>Authorize by OAuth token</b> is <i>On</i> .  Optionally extends the time-to-live for simple OAuth tokens (in seconds). Gives users a short window to accept calls after their credentials expire. However, it increases the potential security exposure.	0 seconds

**Table 6 MRA access control values applied by the upgrade**

Option	Value after upgrade	Previously on...	Now on...
Authentication path	Pre-upgrade setting is applied  <b>Notes:</b>  <b>SSO mode=Off</b> in X8.9 is two settings in X8.10: <ul style="list-style-type: none"><li>■ <b>Authentication path=UCM/LDAP</b></li><li>■ <b>Authorize by user credentials=On</b></li></ul> <b>SSO Mode=Exclusive</b> in X8.9 is two settings in X8.10: <ul style="list-style-type: none"><li>■ <b>Authentication path=SAML SSO</b></li><li>■ <b>Authorize by OAuth token=On</b></li></ul> <b>SSO Mode=On</b> in X8.9 is three settings in X8.10: <ul style="list-style-type: none"><li>■ <b>Authentication path=SAML SSO/and UCM/LDAP</b></li><li>■ <b>Authorize by OAuth token=On</b></li><li>■ <b>Authorize by user credentials=On</b></li></ul>	Both	Cisco VCS Control
Authorize by OAuth token with refresh	Off	–	Cisco VCS Control
Authorize by OAuth token (previously SSO Mode)	Pre-upgrade setting is applied	Both	Cisco VCS Control
Authorize by user credentials	Pre-upgrade setting is applied	Both	Cisco VCS Control
Check for internal authentication availability	No	Cisco VCS Expressway	Cisco VCS Control
Identity providers: Create or modify IdPs	Pre-upgrade setting is applied	Cisco VCS Control	Cisco VCS Control (no change)

Upgrading to X8.10.4

**Table 6 MRA access control values applied by the upgrade (continued)**

Option	Value after upgrade	Previously on...	Now on...
Identity providers: Export SAML data	Pre-upgrade setting is applied	Cisco VCS Control	Cisco VCS Control (no change)
Allow Jabber iOS clients to use embedded Safari	No	Cisco VCS Expressway	Cisco VCS Control
SIP token extra time to live	Pre-upgrade setting is applied	Cisco VCS Control	Cisco VCS Control (no change)

## 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. Select **Log analysis**.
4. Upload your log file(s).
5. Select the log files you want to analyze.
6. Click **Run Analysis**.

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](http://www.cisco.com/go/offices).

© 2017-2018 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](http://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)