Cisco TelePresence Video Communication Server X12.7

Release Notes

First Published: December 2020

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

Change History

Table 1 Release Notes Change History

Date	Change	Reason
December 2020	First publication for X12.7.	X12.7
August 2020	Updates for maintenance release.	X12.6.2
July 2020	Remove misleading section about issues with software downgrade (which is not supported).	Document correction
July 2020	Updates for maintenance release. Also clarify endpoint requirements for OAuth token authorization.	X12.6.1
June 2020	First publication for X12.6.	X12.6

Supported Platforms

Table 2 Cisco VCS Platforms Supported in this Release

Platform name	Serial Numbers	Scope of software version support
Small VM (OVA)	(Auto-generated)	X8.1 onwards For VCS, support for versions after X8.11.x is for maintenance and bug fixing purposes only. New features are not supported.
Medium VM (OVA)	(Auto-generated)	X8.1 onwards For VCS, support for versions after X8.11.x is for maintenance and bug fixing purposes only. New features are not supported.
Large VM (OVA)	(Auto-generated)	X8.1 onwards For VCS, support for versions after X8.11.x is for maintenance and bug fixing purposes only. New features are not supported.
CE1100 (Cisco VCS pre-installed on UCS C220 M4L)	52D######	Not supported (after X12.5.x)
CE1000 (Cisco VCS pre-installed on UCS C220 M3L)	52B######	Not supported (after X8.10.x)
CE500 (Cisco VCS pre-installed on UCS C220 M3L)	52C######	Not supported (after X8.10.x)

Notices Relating to VCS Product Support

Cisco has now announced **end-of-sale and end-of-life** dates for the Cisco TelePresence Video Communication Server (VCS) product. Details are available at https://www.cisco.com/c/en/us/products/collateral/unified-communications/telepresence-video-communication-server-vcs/eos-eol-notice-c51-743969.html

Notices Relating to Hardware Support for CE1100, CE1000, and CE500 Appliances

This section applies to **hardware** support services only.

CE500 and CE1000 appliances - advance notice of hardware service support to be withdrawn

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

CE1100 appliance - end of sale from 13th November 2018 and advance notice of hardware service support to be withdrawn

As of 13 November 2018, you cannot order the CE1100 appliance from Cisco. Cisco will withdraw hardware support services for the appliance in a future release. See the End-of-sale announcement for other important dates in the lifecycle of this platform.

Interoperability and Compatibility

Product Compatibility Information

Detailed matrices

Interoperability test results for Cisco VCS and other Cisco Telepresence products are available here: https://tp-tools-web01.cisco.com/interop/

A compatibility matrix for products in the Cisco Collaboration Systems Release (CSR) set is available here: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/unified/communications/system/Compatibility/CSR-Compatibility-Matrix-InteractiveHTML.html

Mobile and Remote Access

Information about compatible products for MRA specifically, is provided in version tables for infrastructure products and for endpoints in the *Expressway MRA Deployment Guide*.

Which Cisco VCS Services Can Run Together?

The *Cisco Expressway Administrator Guide* 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.

Withdrawn or Deprecated Features and Software

The Cisco VCS product set is under continuous review and features are sometimes withdrawn from the product or deprecated to indicate that support for them will be withdrawn in a subsequent release. This table lists the features that are currently in deprecated status or have been withdrawn since X12.5.

Table 3 Deprecated and withdrawn features

Feature / Software	Status
VMware ESXi6.0 (VM-based deployments)	Deprecated
Cisco Jabber Video for TelePresence (Movi) Note: Relates to Cisco Jabber Video for TelePresence (works in conjunction with Cisco VCS for video communication) and not to the Cisco Jabber soft client that works with Unified CM.	Deprecated
Findme device/location provisioning service - Cisco TelePresence FindMe/Cisco TelePresence Management Suite Provisioning Extension (Cisco TMSPE)	Deprecated
Cisco VCS Starter Pack	Deprecated
Smart Call Home preview feature	Withdrawn X12.6.2
Cisco VCS built-in forward proxy	Withdrawn X12.6.2
Using Cisco VCS as a connector for Cisco Webex Hybrid Services	Withdrawn X12.6
Cisco Advanced Media Gateway	Withdrawn X12.6
VMware ESXi5.x (VM-based deployments)	Withdrawn X12.5

New Features do not Apply to Cisco VCS

New features from software version X12.5 and later **are not supported for the Cisco VCS**, and apply only to the Cisco Expressway Series. For Cisco VCS systems, this version is provided for maintenance and bug fixing purposes only, which includes support for any security enhancements, alarm-based email notifications, and option key changes.

Related Documentation

Table 4 Links to Related Documents and Videos

Support videos	Videos provided by Cisco TAC engineers about certain common Cisco VCS configuration procedures are available on the Expressway/VCS Screencast Video List page (search for "Expressway videos")
Installation - virtual machines	*Cisco Expressway Virtual Machine Installation Guide* on the Expressway installation guides page
Installation - physical appliances	*Cisco Video Communication Server CE1100 Appliance Installation Guide* on the VCS installation guides page
Basic configuration for single-box systems	*Cisco Expressway Registrar Deployment Guide* on the Expressway configuration guides page
Basic configuration for paired-box systems (firewall traversal)	*Cisco Expressway-E and Expressway-C Basic Configuration Deployment Guide* on the Expressway configuration guides page
Administration and maintenance	*Cisco TelePresence VCS Administrator Guide* on the VCS maintain and operate guides page
Clustering	*Cisco Expressway Cluster Creation and Maintenance Deployment Guide* on the Expressway configuration guides page
Certificates	*Cisco Expressway Certificate Creation and Use Deployment Guide* on the Expressway configuration guides page
Ports	*Cisco Expressway IP Port Usage Configuration Guide* on the Expressway configuration guides page
Unified Communications	*Mobile and Remote Access Through Cisco Expressway* on the Expressway configuration guides page
Cisco Meeting Server	*Cisco Meeting Server with Cisco Expressway Deployment Guide* on the Expressway configuration guides page *Cisco Meeting Server API Reference Guide* on the Cisco Meeting Server programming guides page Other Cisco Meeting Server guides are available on the Cisco Meeting Server configuration guides page
Cisco Webex Hybrid Services	Hybrid services knowledge base
Cisco Hosted Collaboration Solution (HCS)	HCS customer documentation

Table 4 Links to Related Documents and Videos (continued)

Microsoft infrastructure	*Cisco Expressway with Microsoft Infrastructure Deployment Guide* on the Expressway configuration guides page *Cisco Jabber and Microsoft Skype for Business Infrastructure Configuration Cheatsheet* on the Expressway configuration guides page
Rest API	*Cisco Expressway REST API Summary Guide* on the Expressway configuration guides page (high-level information only as the API is self-documented)
Multiway Conferencing	*Cisco TelePresence Multiway Deployment Guide* on the Expressway configuration guides page

Features and Changes in X12.7

Security Enhancements

Various security-related improvements apply in this release as part of ongoing security enhancements. Much of this is behind the scenes, but some changes affect the user interfaces or configuration:

- More services are now configured by default on Expressway to require TLS 1.2 as the minimum TLS version (see below for details).
- SMTP mail-based services now require TLS certificate-based verification. This change primarily affects the alarm-based email notification feature (see below for details).
- An additional password check is now performed if the "Enforce strict passwords" feature is enabled (**Users > Password security** page). From X12.7, if the account holder tries to use the same letters as their username in their password – in straight or reverse order, and in lower or upper case – an error message is displayed.
  Note: The strict passwords feature applies to the local authentication database, and administrator accounts and FindMe user accounts managed locally in Expressway, but does not apply to LDAP and externally stored credentials.

Extension of TLS 1.2 as Default Minimum Version

The default minimum TLS version is now TLS 1.2 for the additional services in X12.7, as listed in the table. The default version – and associated ciphers – can be configured to a lower version (not recommended) from the **Maintenance > Security > Ciphers** page.

Service	Configuration setting
Certificate Checker	*HTTPS minimum TLS version*
Cisco Meeting Server discovery	*Reverse proxy minimum TLS version*
LDAP	*LDAP minimum TLS version*
SMTP mail client (TLS certificate-based authentication from X12.7)	*SMTP minimum TLS version*
TMS Provisioning Service	*TMS provisioning minimum TLS version*
UC server discovery (AXL query)	*UC server discovery minimum TLS version*

TLS Changes – Impact for TMS and CMS

From X12.7, Cisco TMS and Cisco Meeting Server are included in the services for which the default minimum TLS version is TLS 1.2. This means that if any Cisco TMS or Cisco Meeting Servers are deployed with TLS 1.1 or lower, the TLS handshake will fail.

TLS Changes – Impact for LDAP

From X12.7, LDAP is included in the services for which the default minimum TLS version is TLS 1.2. This means that if any LDAP servers are deployed with TLS 1.1 or lower, only local administrators will be able to sign in, and the TLS handshake will fail. **Remote administrators will be unable to sign in until such time as the LDAP server supports TLS 1.2** (and the **Ciphers** page is updated to match).

Configuration change on upgrade – "Remote-only" automatically set to "Both"

This change applies if you currently (before upgrading to this release) specify "*Remote only*" for the administrator authentication source setting on the **Users > LDAP configuration** page. To avoid remote administrators being

unintentionally locked out of the Expressway, on upgrade to X12.7 or later, **this setting is automatically changed to "Both"**.

After the upgrade is complete, if you want to limit administrator sign ins again so that only remote administrators may authenticate:

1. Verify that the LDAP connection status is "*Available*".
2. On the **Users > LDAP configuration** page, reconfigure the administrator authentication source back to "*Remote only*".

TLS Changes – Impact for SMTP

From X12.7, Expressway requires SMTP services to use TLS 1.2 certificate-based verification. These configuration prerequisites must be in place, else **alarm-based email notifications (and any other SMTP-based functions) will fail**:

- As the SMTP server certificate gets validated by the client, its IP address and/or FQDN must be in the certificate's CN/SAN.
- The SMTP server certificate issuer needs to be imported into the Cisco VCS trusted CA certificate list (**Maintenance > Security > Trusted CA Certificate**).

CBC Ciphers Removed from SSH Default Configuration

As part of our ongoing security enhancements, CBC-mode ciphers are no longer included in the system's default cipher configuration for SSH. The upgrade will automatically change the default values to remove the CBC ciphers - aes129-cbc, aes-256-cbc, aes192-cbc. If you need these ciphers (not recommended) you can use the *xconfiguration Ciphers sshd_ciphers* command to reconfigure them.

Virtualized Systems – Later VM Hardware Version

This item applies to Expressways running as virtualized systems. Expressway X12.7 is compatible with VM hardware version 11.

Virtualized Systems – ESXi 7.0 for Large/Medium VMs

This item applies to Cisco VCSs running as virtualized systems. Cisco VCS X12.7 is compatible with VMware ESXi version 7.0.

Virtualized Systems – ESXi 6.0 now Deprecated

This item applies to Cisco VCSs running as virtualized systems. VMware ESXi6.0 is now deprecated for Cisco VCS systems.

Ongoing Removal of Unsupported Functions from UI

To enhance usability and consistency we are removing discontinued functions and features from the user interface. Details per release are in Withdrawn or Deprecated Features and Software, page 6

There are no changes in this respect for the X12.7 release.

Other Changes in this Release

The Connection Manager log has been improved.

REST API Changes

The REST API for Cisco VCS is available to simplify remote configuration. For example by third party systems such as Cisco Prime Collaboration Provisioning. We add REST API access to configuration, commands, and status information as new features are added, and also selectively retrofit the REST API to some features that were added in earlier versions of Cisco VCS.

The API is self-documented using RAML, and you can access the RAML definitions at `https://<ip address>/api/raml`. A high-level summary of how to access and use the API is provided in the *Cisco Expressway REST API Summary Guide* on the VCS configuration guides page.

Configuration APIs	API introduced in version
Clustering	X8.11
Smart Call Home	X8.11
Microsoft Interoperability	X8.11
B2BUA TURN Servers	X8.10
Admin account	X8.10
Firewall rules	X8.10
SIP configuration	X8.10
Domain certificates for Server Name Identification	X8.10
MRA expansion	X8.9
Business to business calling	X8.9
MRA	X8.8

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 X12.7

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 the Cisco VCS Expressway is correctly licensed to ensure continuity of service with future upgrades.

Limitations

Some Cisco VCS Features are Preview or Have External Dependencies

We aim to provide new Cisco VCS 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. If customers might still benefit from using the feature, we mark it 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. Cisco VCS features which are provided in preview status only in this release, are listed in the Feature History table earlier in these notes.

Unsupported Functionality

- Currently, if one Cisco VCS node in a clustered deployment fails or loses network connectivity for any reason, or if the Unified CM restarts, all active calls going through the affected node will fail. The calls are not handed over to another cluster peer. This is not new behavior in X12.5.x, but due to an oversight it was not documented in previous releases. Bug ID CSCtr39974 refers.
- Cisco VCS does not terminate DTLS. We do not support DTLS for securing media and SRTP is used to secure calls. Attempts to make DTLS calls through Cisco VCS will fail. The DTLS protocol is inserted in the SDP but only for traversing the encrypted iX protocol.
- Cisco VCS does not support the SIP UPDATE method (RFC 3311), and 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.

Cisco VCS TURN does Not Operate as a STUN Server

From X12.6.1, due to security enhancements, the Cisco VCS Expressway TURN server no longer functions as a generic STUN server and will not accept unauthenticated STUN binding requests.

This leads to the following scenarios:

- Scenario A: If you use the B2BUA as a TURN client for Microsoft interoperability (as described in the *Cisco Expressway with Microsoft Infrastructure Deployment Guide*) the B2BUA will not send any STUN binding requests to the TURN server to check if it is alive or not. This means that from Cisco VCS X12.6.1, the B2BUA may try to use a TURN server that is not reachable and hence that **calls may fail**.
- Scenario B: If you use Meeting Server WebRTC with Expressway (and Expressway-E is configured as a TURN server) before you install Cisco VCS X12.6.1 or later, first upgrade the Meeting Server software to version 3.0 or to a compatible maintenance release in version 2.9.x or 2.8.x. Bug ID CSCvv01243 refers. This requirement is because other Meeting Server versions use STUN bind requests towards the TURN server on Cisco VCS Expressway (For more information about Cisco VCS Expressway TURN server configuration, see the *Cisco Expressway Web Proxy for Cisco Meeting Server Deployment Guide*.) .

Cisco Webex Hybrid Call Service

Expressway X12.6 and later does not work for hosting the Call Connector software that is required in a Hybrid Call Service deployment and you need to use an earlier supported version for the Expressway connector host. See the Hybrid Call Service known issues and Expressway version support documentation on https://help.webex.com for more information.

Product License Registration - Issue with Converting to Smart Licensing

This item applies if you want to convert existing Expressway licenses (RMS, Desktop, or Room) to Smart Licensing entitlements. In this case do not use the option in the Cisco Product License Registration portal to partially convert just some of the licenses. Due to a known issue, if you opt to convert only some licenses, the system automatically forfeits/removes the remaining licenses as well. So the licenses that are not converted are also removed, and a licensing case will be required to retrieve them.

To avoid this happening, please ensure that the **Quantity to Convert** field is the same value as the **Quantity Available** field; this is the default when you open the page.

Static NAT for Clustered Systems

From X12.5.5, support for static NAT functionality on TURN is extended to clustered systems (support for standalone systems was introduced in X12.5.3). However, peers which are configured as TURN servers must be reachable using the private addresses for their corresponding public interfaces.

MRA Limitations

If you use Cisco VCS for Mobile and Remote Access (MRA), some unsupported features and limitations currently exist. Details are provided in the *Mobile and Remote Access Through Cisco Expressway* guide, *Limitations and Feature Support* chapter.

For details of which 7800/8800 Series phones and other endpoints support MRA, see the *MRA Requirements* section of the *Mobile and Remote Access Through Cisco Expressway* guide.

SIP UPDATE for session refresh support over MRA has some limitations. For example, the following features that rely on the SIP UPDATE method (RFC 3311) will fail:

- Request to display the security icon on MRA endpoints for end-to-end secure calls.
- Request to change the caller ID to display name or number on MRA endpoints.

MRA IM&P Dual Connection (MRA HA) - Do Not Use

Expressway X12.7 can support IM&P dual connection mode. However, please do not use this feature as it is not yet implemented throughout the wider solution.

MRA OAuth Token Authorization with Endpoints / Clients

In standard MRA mode (no ICE) regardless of any MRA access policy settings configured on Unified CM, Cisco Jabber users will be able to authenticate by username and password or by traditional single sign-on in the following case:

- You have Jabber users running versions before 11.9 (no refresh token support) and Cisco VCS is configured to allow non-token authentication.

In ICE passthrough mode, the ICE MRA call path must be encrypted end-to-end (see *Signaling Path Encryption Between Expressway-C and Unified CM* in the *Expressway MRA Deployment Guide*). Typically for end-to-end encryption, Unified CM must be in mixed mode for physical endpoints. For Jabber clients however, you can achieve the end-to-end encryption requirement by leveraging SIP OAuth with Unified CM clusters that are not in mixed mode. Note that you must enable SIP OAuth if the Unified CM is not in mixed mode, but SIP OAuth is not required for Jabber if you're able to register using standard secure profiles.

More information is in the *Configure MRA Access Control* section of the *Expressway MRA Deployment Guide* and in the *Deploying OAuth with Cisco Collaboration Solution Release 12.0* White Paper.

Spurious Alarms when Adding or Removing Peers in a Cluster

When a new peer is added to a cluster, the system may raise multiple 20021 Alarms (*Cluster communication failure: Unable to establish...*) even if the cluster is in fact correctly formed. The alarms appear on the existing peers in the cluster. The unnecessary alarms are typically lowered after at least 5 minutes elapses from the time that the new peer is successfully added.

These alarms also occur if a peer is removed from a cluster. This is generally valid alarm behavior in the case of removing a peer. However, as in the case of adding a peer, the alarms may not be lowered for 5 minutes or more.

Virtual Systems

- This issue applies to Cisco VCSs running as virtualized systems with certain ESXi versions using VMWare vCenter 7.0.x. It was found during testing using VMWare vCenter 7.0.1 with ESXi 6.7.0 to deploy a VCS OVA. The *Ready to complete* final page of the *Deploy OVF Template* wizard displays template values instead of the actual values entered on the earlier wizard pages. The issue is cosmetic, and when you click "FINISH" the OVA will deploy as expected using the entered values. Bug ID CSCvw64883 refers.
- Video calling capacity may be restricted if the ESXi Side-Channel-Aware Scheduler is enabled, and CPU load exceeds 70%.
- With physical Cisco VCS appliances, the **Advanced Networking** feature 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).

Medium Appliances with 1 Gbps NIC - Demultiplexing Ports

If you upgrade a Medium appliance with a 1 Gbps NIC to X8.10 or later, Cisco VCS automatically converts the system to a Large system. This means that Cisco VCS Expressway listens for multiplexed RTP/RTCP traffic on the default demultiplexing ports for Large systems (36000 to 36011) and not on the demultiplexing ports configured for Medium systems. In this case, the Cisco VCS Expressway drops the calls because ports 36000 to 36011 are not open on the firewall.

Workaround

From X8.11.4 you can manually change the system size back to Medium, through the **System > Administration settings** page (select *Medium* from the **Deployment Configuration** list).

Before X8.11.4, the workaround is to open the default demultiplexing ports for Large systems on the firewall.

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*.

XMPP Federation-Behavior on IM&P Node Failure

If you use XMPP external federation, be aware that if an IM and Presence Service node fails over to a different node after an outage, the affected users are not dynamically moved to the other node. Cisco VCS does not support this functionality, and it has not been tested.

Cisco Webex Calling May Fail with Dual-NIC Cisco VCS

This issue applies if you deploy Cisco VCS with a dual-NIC Cisco VCS Expressway. Cisco Webex Calling requests may fail if the same (overlapping) static route applies to both the external interface and the interface with the Cisco VCS Control. This is due to current Cisco VCS Expressway routing behavior, which treats Webex INVITES as non-NAT and therefore extracts the source address directly from the SIP Via header.

We recommend that you make static routes as specific as possible, to minimize the risk of the routes overlapping, and this issue occurring.

Microsoft Federation with Dual Homed Conferencing-SIP Message Size

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. It's likely that you will need a greater value for larger conferences (that is, from around nine or more participants upwards). Defined via **SIP max size** on **Configuration > Protocols > SIP**.

Intradomain Microsoft Interop with Expressway and Cisco Meeting Server

If you use Meeting Server for Microsoft interoperability, a limitation currently applies to the following intradomain/intracompany scenario:

*You deploy separate Microsoft and standards-based SIP networks in a **single domain** and in a configuration that has an Cisco VCS Expressway **directly facing** a Microsoft front end server (because you use internal firewalls between subnetworks, or for any other reason). For example, Cisco Unified Call Manager in one (sub)network and Microsoft in a second (sub)network, inside the same domain.*

In this case we do not generally support Microsoft interoperability between the two networks, and calls between Meeting Server and Microsoft will be rejected.

Workaround

If you are not able to deploy the intradomain networks without an intervening VCS Expressway (you cannot configure Meeting Server <> VCS Control <> Microsoft), a workaround is to deploy a VCS-C in each subnet, with a VCS-E to traverse between them. That is:

Meeting Server <> VCS Control <> Firewall <> VCS Expressway<> Firewall <> VCS Control <> Microsoft

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. Bug ID CSCvf78728 refers.

Upgrading Cisco VCS to X12.7

This section describes how to install the software on Cisco VCS using the web user interface, which is the method we recommend. If you prefer to use a secure copy program such as SCP or PSCP to do the install, please use the *Administrator Guide* instead.

Summary

Table 5 Summary of tasks in a typical upgrade process

Stage	Task	Where…
1	Review the *Prerequisites and Software Dependencies* and *Before You Begin* sections below	Release Notes
2	Back up the system	**Maintenance > Backup and restore**
3	Enable maintenance mode and wait for current calls and registrations to end	**Maintenance > Maintenance mode**
4	Upload the new software image ("**Upgrade**" option)	**Maintenance > Upgrade**
5	Install the new software ("**Continue with upgrade**" option)	**Maintenance > Upgrade**
6	Reboot	From the **Upgrade** page
7	In clustered deployments repeat for each peer in sequence	-

Prerequisites and Software Dependencies

This section has important information about 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.

Cisco VCS systems before X8.11.4 need a two-stage upgrade

If you are upgrading a system which is running software earlier than version X8.11.4, you must first upgrade to an **intermediate release** before you install X12.7 software (this requirement applies to all upgrades to X8.11.x and later versions). Depending on the existing system version, the upgrade will fail. We recommend upgrading to X8.11.4 as the intermediate release.

Is a release key needed?

If you are upgrading to a new major release, for example from X9.x to X12.x, you first need a new release key from Cisco. The key is required during the upgrade process. You can get a release key from the licensing portal https://slexui.cloudapps.cisco.com/SWIFT/LicensingUI/Quickstart. Select **Licenses > Get Licenses > Telepresence software release key** and enter the serial number of the Cisco VCS VM or physical appliance. If you don't have the appropriate contract to get a key, you can use the portal to request an upgrade license or to raise a case with licensing support.

All deployments

If you are upgrading from X12.6 or X12.6.1 and use the alarm-based email notifications feature, please note that in X12.6.2 the email ID length is limited to 254 characters maximum. Before you upgrade make sure that all destination email IDs are no longer than 254 characters.

We do not support downgrades. Do not install a previous Cisco VCS version onto a system that is running a newer version; the system configuration will be lost.

Note that from X8.11.x, when the system restarts after the upgrade it uses a new encryption mechanism. This is due to a unique root of trust for every software installation that was introduced in that release.

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: Because certificate validation was tightened up in X8.8, you must verify the following items to avoid validation failures:
  - Try the secure traversal test before and after upgrade (**Maintenance > Security > Secure traversal test**) to validate TLS connections.
  - If Unified Communications nodes are deployed, do they use valid certificates that were issued by a CA in the Cisco VCS Control trust list?
  - If you use 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 trusted CA list unique? Remove any duplicates.
  - If **TLS verify mode** is enabled on connections to other infrastructure (always on by default for Unified Communications traversal zone, and optional for zones to Unified Communications nodes), make sure 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, you need 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 system hostnames and IP addresses, complex deployments like MRA may not work as expected after the 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. By default, TLS verification is not enforced after the upgrade, and an alarm will remind you to enforce it.

How and when rebooting is necessary as part of the upgrade

Upgrading the *System platform* component is a two-stage process. First, the new software image is uploaded onto the Cisco VCS. At the same time, the current configuration of the system is recorded, so that this can be restored after the upgrade. During this initial stage the system will continue running on its existing software version, and all normal system processes will continue.

The second part of the upgrade involves rebooting the system. It is only during the reboot that the Cisco VCS installs the new software version and restores the previous configuration. Rebooting causes all current calls to terminate, and all current registrations to be ended. This means that you can upload the new software at any time, and then wait until a convenient moment (for example, when no calls are taking place) to switch to the new version by rebooting the system. Any **configuration changes made between the software upload and the reboot will be lost when the system restarts** with the new software version.

Upgrades for components other than the *System platform* do not involve a system reboot, although the services provided by that component are temporarily stopped while the upgrade process completes.

Deployments that use MRA

This section only applies if you use the Cisco VCS for MRA (mobile and remote access with Cisco Unified Communications products).

- Minimum versions of Unified Communications infrastructure software apply - some versions of Unified CM, IM and Presence Service, and Cisco Unity Connection have been patched with CiscoSSL updates. Before you upgrade Cisco VCS check that you are running the minimum versions listed in the *Mobile and Remote Access Through Expressway Deployment Guide*.

  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.

- Cisco VCS Control and Cisco VCS Expressway **should both be upgraded** in the same upgrade "window"/timescale (this is also a general recommendation for non-MRA deployments). We don't recommend operating with Cisco VCS Control and Cisco VCS Expressway on different versions for an extended period.
- This item 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. Bug ID CSCvh97495 refers.
  - TC7.3.11
  - CE8.3.3
  - CE9.1.2

From X8.10.x, the MRA authentication (access control) settings are configured on Cisco VCS Control and not on Cisco VCS Expressway as in earlier releases, and default values are applied if it is not possible to retain the existing settings. To ensure correct system operation, after the upgrade reconfigure the access control settings on the Cisco VCS, as described later in these instructions.

Deployments that use FIPS mode cryptography

If the Cisco VCS has FIPS mode enabled, after the upgrade, manually change the default SIP TLS Diffie-Hellman key size from the default 1024 bits, to 2048 or greater, as described later in these instructions

Deployments that use X8.7.x or earlier with Cisco Unified Communications Manager IM and Presence Service 11.5(1)

X8.7.x (and earlier versions) of Cisco VCS are not interoperable with Cisco Unified Communications Manager IM and Presence Service 11.5(1) and later. This is caused by a deliberate change in that version of IM and Presence Service, which has a corresponding change in Cisco VCS X8.8 and later. To ensure continuous interoperability, upgrade the Cisco VCS systems before you upgrade the IM and Presence Service systems. The following error on Cisco VCS is a symptom of this issue: *Failed Unable to Communicate with <IM&P node address>. AXL query HTTP error "'HTTPError:500'"*

Deployments that use Cisco Webex Hybrid Services

The Management Connector must be up to date before you upgrade Cisco VCS. Authorize and accept any Management Connector upgrades advertised by the Cisco Webex cloud before you try to upgrade Cisco VCS. Failure to do so may cause issues with the connector after the upgrade. For details about which versions of Cisco VCS are supported for hybrid connector hosting, see Connector Host Support for Cisco Webex Hybrid Services

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

- Do the upgrade when the system has low levels of activity.
- A system upgrade needs a system reboot to complete the process. The reboot will terminate any active calls and registrations.
- For clustered systems, allocate enough time to upgrade all peers in the same upgrade "window". The cluster will not re-form correctly until the software versions match on all peers
- Check the Alarms page (**Status > Alarms**) and make sure that all alarms are acted upon and cleared. Do this for each peer if you are upgrading a cluster.
- If you are upgrading a VM-based system, use the standard *.tar.gz* software image file. The *.ova* file is only needed for the initial install of Cisco VCS software onto VMware.
- If you use the Cisco VCS for MRA and you upgrade from X8.9.x or earlier to X8.10 or later, note your MRA authentication settings before you upgrade. From version X8.10 the MRA authentication (access control) settings moved from the Cisco VCS Expressway to the Cisco VCS Control. The upgrade does not preserve the existing Cisco VCS Expressway settings, so after the upgrade you need to review them on the Cisco VCS Control and adjust as necessary for your deployment. To access existing MRA authentication settings:
  a. 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)
  b. If **Single Sign-on support** is set to On or Exclusive, also note the current values of these related fields:
     - **Check for internal authentication availability**
     - **Allow Jabber iOS clients to use embedded Safari**
- Make sure that all relevant tasks in Prerequisites and Software Dependencies, page 17 are complete.

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

In all cases 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.** For some services such as Mobile and Remote Access, we *require* both systems to run the same version.

However, we do support a traversal zone link from one Cisco VCS system to another that is running the previous feature release of Cisco VCS (for example, from an X12.6 system to an X12.5 system). This means that you do not have to simultaneously upgrade your Cisco VCS Control and Cisco VCS Expressway systems.

Process to Upgrade a Standalone System

Do not use this process if you are upgrading a clustered Cisco VCS; instead use the process to upgrade a clustered system.

1. Sign in to the Cisco VCS web user interface as *admin*.
2. Back up the Cisco VCS system before you upgrade (**Maintenance > Backup and restore**).
3. Enable maintenance mode so that Cisco VCS does not process any new incoming calls (**Maintenance > Maintenance mode**). Existing calls continue until the call is terminated.
4. Wait for all calls to clear and registrations to timeout.

   To manually remove any calls or registrations that don't clear automatically, use the **Status > Calls** page or the **Status > Registrations > By device** page respectively (SIP calls may not clear immediately).

   Note: You can leave the registration for Conference Factory (if enabled) – this will not be the source of calls, and even if deleted will not roll over to another peer, as other peers have their own Conference Factory registration.
5. Go **Maintenance > Upgrade** to access the **Upgrade** page.
6. Click **Browse** and select the software image file for the component you want to upgrade.
   The Cisco VCS automatically detects which component you are upgrading based on the selected software image file.
7. Click **Upgrade**. This step uploads the software file but does not install it. The upload may take a few minutes to finish.
8. For upgrades to the **System platform** component, the **Upgrade confirmation** page is displayed:
   a. Check the following details:
      - **New software version** number is as expected.
      - **MD5 hash** and **SHA1 hash** values match the values displayed on the cisco.com page, where you downloaded the software image file.
   b. Click **Continue with upgrade**. This step installs the new software.
      The **System upgrade** page opens and displays a progress bar while the software installs.
      A summary of any active calls and registrations is displayed when the software completes installing (the calls and registrations will be lost when you reboot the system in the next step).
   c. Click **Reboot system**. Any configuration changes made between uploading the software tar file and rebooting, will be lost when the system restarts.

      Sometimes the web browser interface times out during the restart process, after the progress bar reaches the end. This may occur if the Cisco VCS carries out a disk file system check – approximately once every 30 restarts.

      After the reboot is complete the **Login** page is displayed.
9. For upgrades to other components (not System platform) the software is automatically installed and no reboot is required.

What Next?

If you don't use MRA, the upgrade is now complete, and the Cisco VCS configuration should be as expected. The **Overview** and **Upgrade** pages show the upgraded software version numbers.

If you do use MRA, and you are upgrading from X8.9.x or earlier, reconfigure your MRA access control settings as described in Appendix 1: Post-Upgrade Tasks for MRA Deployments, page 27

If you have components that require option keys to enable them, do this from the **Maintenance > Option keys** page.

If the Cisco VCS has FIPS mode enabled (that is, it's a FIPS140-2 cryptographic system) then from X12.6 you must manually change the default SIP TLS Diffie-Hellman key size from the default 1024 bits, to 2048 or greater. To do this type the following command in the Cisco VCS command line interface (change the value in the final element if you

want a key size higher than 2048): *xconfiguration SIP Advanced SipTlsDhKeySize: "2048"*
This step does **not** apply to most systems. It only affects systems with advanced account security configured and FIPS enabled.

Process to Upgrade a Clustered System

CAUTION: To avoid the risk of configuration data being lost and to maintain service continuity, UPGRADE THE PRIMARY PEER FIRST and then upgrade the subordinate peers ONE AT A TIME in sequence.

We recommend upgrading the Expressway-E cluster first, followed by the Expressway-C (in each case start with the primary peer). This ensures that when Expressway-C starts a new traversal session toward Expressway-E, the Expressway-E is ready to process it. Starting with the primary peer, upgrade the cluster peers in sequence as follows:

1. Sign in to the Cisco VCS web user interface as *admin*.
2. Back up the Cisco VCS before you upgrade (**Maintenance > Backup and restore**).

   Note: If the cluster peers are running different versions of the Cisco VCS, do not make any configuration changes other than the settings required to upgrade. The cluster does not replicate any configuration changes to the subordinate peers that are running on different versions from the primary Cisco VCS.
3. Enable maintenance mode so that the peer does not process any new incoming calls (**Maintenance > Maintenance mode**). Existing calls continue until the call is terminated. Other peers in the cluster continue to process calls.
4. Wait for all calls to clear and registrations to timeout.

   To manually remove any calls or registrations that don't clear automatically, use the **Status > Calls** page or the **Status > Registrations > By device** page respectively (SIP calls may not clear immediately).

   Note: You can leave the registration for Conference Factory (if enabled) – this will not be the source of calls, and even if deleted will not roll over to another peer, as other peers have their own Conference Factory registration.
5. Go **Maintenance > Upgrade** to access the **Upgrade** page.
6. Click **Browse** and select the software image file for the component you want to upgrade. The Cisco VCS automatically detects which component you are upgrading based on the selected software image file.
7. Click **Upgrade**. This step uploads the software file but does not install it. The upload may take a few minutes to finish.
8. For upgrades to the **System platform** component, the **Upgrade confirmation** page is displayed:
   a. Check the following details:
      - **New software version** number is as expected.
      - **MD5 hash** and **SHA1 hash** values match the values displayed on the cisco.com page, where you downloaded the software image file.
   b. Click **Continue with upgrade**. This step installs the new software.
      The **System upgrade** page opens and displays a progress bar while the software installs.
      A summary of any active calls and registrations is displayed when the software completes installing (the calls and registrations will be lost when you reboot the system in the next step).
   c. Click **Reboot system**. Any configuration changes made between uploading the software tar file and rebooting, will be lost when the system restarts.

      Sometimes the web browser interface times out during the restart process, after the progress bar reaches the end. This may occur if the Cisco VCS carries out a disk file system check – approximately once every 30 restarts.

      Ignore any cluster-related alarms and warnings that occur during the upgrade process, such as cluster communication failures or cluster replication errors. These are expected and will resolve when all cluster peers are upgraded and after cluster data synchronization (typically within 10 minutes of the complete upgrade).

      After the reboot is complete the **Login** page displays.
9. For upgrades to other components (not the System platform) the software is automatically installed and no reboot is required.
10. Repeat the previous steps for each peer in sequence until all peers are on the new software version.

What Next?

1. Verify the new status of each Cisco VCS (including the primary):
   a. Go to **System > Clustering** and check that the cluster database status reports as **Active**.
   b. Check the configuration for items from the System, Configuration, and Application menus.
2. Backup the Cisco VCS again (**Maintenance > Backup and restore**).
3. If you use MRA, and you are upgrading from X8.9.x or earlier, reconfigure the MRA access control settings as described in Appendix 1: Post-Upgrade Tasks for MRA Deployments, page 27
4. If you have components that require option keys to enable them, do this from the **Maintenance > Option keys** page.
5. If the Cisco VCS has FIPS mode enabled (that is, it's a FIPS140-2 cryptographic system) then from X12.6 you must manually change the default SIP TLS Diffie-Hellman key size from the default 1024 bits, to 2048 or greater. To do this type the following command in the Cisco VCS command line interface (change the value in the final element if you want a key size higher than 2048): *xconfiguration SIP Advanced SipTlsDhKeySize: "2048"*
   This step does **not** apply to most systems. It only affects systems with advanced account security configured and FIPS enabled.
6. (Optional) If for any reason you want to change the default TLS version, the *Cisco Expressway Certificate Creation and Use Deployment Guide* explains how to set the TLS version on each peer.

The software upgrade on the Cisco VCS cluster is now complete.

Using Collaboration Solutions Analyzer

The *Collaboration Solutions Analyzer* is created by Cisco Technical Assistance Center (TAC) to help you with validating your deployment, and to assist with troubleshooting by analyzing Cisco VCS log files. For example, you can use the Business to Business Call Tester to validate and test calls, including Microsoft interworked calls.

You need a customer or partner account to use the Collaboration Solutions Analyzer.

Getting started

1. If you plan to use the log analysis tool, first collect the Cisco VCS logs.
2. Sign in to https://cway.cisco.com/tools/CollaborationSolutionsAnalyzer/

   From X12.6 you can use the **Analyze log** button on the **Diagnostic logging** page (**Maintenance > Diagnostics**) to open a link to the Collaboration Solutions Analyzer troubleshooting tool.
3. Click the tool you want to use. For example, to work with logs:
   a. Click **Log analysis**.
   b. Upload the log file(s).
   c. Select the files you want to analyze.
   d. Click **Run Analysis**.

      The tool analyzes the log files and displays the information in a format which 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.

Appendix 1: 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 X8.9.x 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 6 Settings for MRA access control

Field	Description	Default
Authentication path	Hidden field until MRA is enabled. Defines how MRA authentication is controlled. *SAML SSO authentication*: Clients are authenticated by an external IdP. *UCM/LDAP basic authentication*: Clients are authenticated locally by the Unified CM against their LDAP credentials. *SAML SSO and UCM/LDAP*: Allows either method. *None*: No authentication is applied. This is the default setting until MRA is first enabled. The "None" option is needed (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". **Do not use it in other cases.**	None before MRA turned on UCM/LDAP after MRA turned on
Authorize by OAuth token with refresh	This option requires self-describing tokens for authorization. It's our recommended authorization option for all deployments that have the infrastructure to support them. 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.	On

Table 6 Settings for MRA access control (continued)

Field	Description	Default
Authorize by OAuth token (previously SSO Mode)	Available if **Authentication path** is *SAML SSO* or *SAML SSO and UCM/LDAP*. 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.	Off
Authorize by user credentials	Available if **Authentication path** is *UCM/LDAP* or *SAML SSO and UCM/LDAP*. Clients attempting to perform authentication by user credentials are allowed through MRA. This includes Jabber, and supported IP phone and TelePresence devices.	Off
Check for internal authentication availability	Available if **Authorize by OAuth token with refresh** or **Authorize by OAuth token** is enabled. The default is No, for optimal security and to reduce network traffic. 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. 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: *Yes*: The *get_edge_sso* 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 *get_edge_sso* request. *No*: 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. 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 *No*. Or select *Yes* 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. **Caution: Setting this to *Yes* has the potential to allow rogue inbound requests from unauthenticated remote clients.** If you specify No for this setting, the Cisco VCS prevents rogue requests.	No

Table 6 Settings for MRA access control (continued)

Field	Description	Default
Identity providers: Create or modify IdPs	Available if **Authentication path** is *SAML SSO* or *SAML SSO and UCM/LDAP*. **Selecting an Identity Provider** Cisco Collaboration solutions use SAML 2.0 (Security Assertion Markup Language) to enable SSO (single sign-on) for clients consuming Unified Communications services. If you choose SAML-based SSO for your environment, note the following: ■ SAML 2.0 is not compatible with SAML 1.1 and you must select an IdP that uses the SAML 2.0 standard. ■ 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. ■ 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. 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: ■ OpenAM 10.0.1 ■ Active Directory Federation Services 2.0 (AD FS 2.0) ■ PingFederate® 6.10.0.4	–
Identity providers: Export SAML data	Available if **Authentication path** is *SAML SSO* or *SAML SSO and UCM/LDAP*. For details about working with SAML data, see SAML SSO Authentication Over the Edge, page 1.	–

Table 6 Settings for MRA access control (continued)

Field	Description	Default
Allow Jabber iOS clients to use embedded Safari	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. This setting optionally allows 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 OAuth deployment. 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. 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.	No
SIP token extra time to live	Available if **Authorize by OAuth token** is *On*. 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 7 MRA access control values applied by the upgrade

Option	Value after upgrade	Previously on…	Now on…
Authentication path	Pre-upgrade setting is applied **Notes:** **SSO mode**=*Off* in X8.9 is two settings in X8.10: ▪ **Authentication path**=*UCM/LDAP* ▪ **Authorize by user credentials**=*On* **SSO Mode**=*Exclusive* in X8.9 is two settings in X8.10: ▪ **Authentication path**=*SAML SSO* ▪ **Authorize by OAuth token**=*On* **SSO Mode**=*On* in X8.9 is three settings in X8.10: ▪ **Authentication path**=*SAML SSO/and UCM/LDAP* ▪ **Authorize by OAuth token**=*On* ▪ **Authorize by user credentials**=*On*	Both	Cisco VCS Control
Authorize by OAuth token with refresh	On	–	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)
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)

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.

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)