Cisco TelePresence Video Communication Server Release Note (X14.0.4)

First Published: 2021-11-24

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1

About the Documentation

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.

Change History

Table 1: Release Notes Change History

Date	Change	Reason
December 2021	First publication for X14.0.4	X14.0.4 release
August 2021	First publication for X14.0.3	X14.0.3 release

Date	Change	Reason
July 2021	First publication for X14.0.2	X14.0.2 release
June 2021	First publication for X14.0.1	X14.0.1 release
May 2021	Included a limitation in MRA Limitations section.	X14.0 release - Republished
April 2021	First publication for X14.0	X14.0 release
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, clarification on 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)

Platform name	Serial Numbers	Scope of software version support
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 Deploying OVA with VMware 7.0 U2

Note This is a known issue in the current release. Deploying X14.0.3 OVA shows "Invalid Certificate" on vCenter 7.0U2 version of VMware, though it shows "Trusted Certificate" in older versions. Refer to this Knowledge Article for more information about the issue.

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 the following link.

Notices Relating to Hardware Support for CE1200, CE1100, CE1000, and CE500 Appliances

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

Important Supply issues with components used in the Expressway CE1200 are delaying orders. In light of the supply issues, we are extending the end of Vulnerability/Security support for the CE1100 by 3 months, that is, from November 14, 2021 to February 14, 2022.

CE1100 appliance - end-of-sale and advance notice of hardware service support withdraw

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.

CE500 and CE1000 appliances - End-of-sale notice

The Cisco Expressway CE500 and CE1000 appliance hardware platforms are no longer supported by Cisco. See the End-of-sale announcement for more details.

Interoperability and Compatibility

Product Compatibility Information

Detailed matrices

Cisco Expressway is standards-based and interoperates with standards-based SIP and H.323 equipment both from Cisco and third parties. For specific device interoperability questions, contact your Cisco representative.

Mobile and Remote Access (MRA)

Information about compatible products for MRA specifically, is provided in version tables for infrastructure products and for endpoints in the Mobile and Remote Access Through Cisco Expressway 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 Expressway 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
Support for Microsoft Internet Explorer browser	Deprecated from X14.0.2
VMware ESXi 6.0 (VM-based deployments)	Deprecated
Cisco Jabber Video for TelePresence (Movi) **Note** Relates to Cisco Jabber Video for TelePresence (works in conjunction with Cisco Expressway 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
Expressway Starter Pack	Deprecated
Smart Call Home preview feature	Withdrawn X12.6.2

Feature / Software	Status
Expressway built-in forward proxy	Withdrawn X12.6.2
Cisco Advanced Media Gateway	Withdrawn X12.6
VMware ESXi 5.x (VM-based deployments)	Withdrawn X12.5

No Support for Ray Baum's Act

Expressway is not an MLTS (Multiline Telephone System). Customers that need to comply with the requirements of Ray Baum's Act should use Cisco Unified Communication Manager in conjunction with Cisco Emergency Responder.

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
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.

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.

Features and Changes in X14.0.4

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.

X14.0.4 release

RedSky E911 Location Services Support in Expressway: As part of this change, Expressway will passthrough SIP headers (needed for RedSky feature) - Geolocation, Geolocation-Routing, and RedSky-CustomerID. The SIP header value for Geolocation will be masked in all Expressway logs for security reasons.

X14.0.3 release

- Cisco has released software updates that addresses the following vulnerabilities.
  - **Remote Code Execution Vulnerability**: A vulnerability in the Web-based management interface of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) can allow an authenticated, remote attacker to execute arbitrary code on the underlying operating system as the *root* user.

    This vulnerability occurs due to incorrect handling of certain crafted software images that are uploaded to the affected device. An attacker can authenticate the system as an administrative user and exploit this vulnerability. The attacker can then upload specific crafted software images to the affected device. A successful exploit can allow the attacker to execute arbitrary code on the underlying operating system as the *root* user.
  - **Image Verification Vulnerability**: A vulnerability in the image verification function of the Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) can allow an authenticated, remote attacker to execute code with internal user privileges on the underlying operating system.

    The vulnerability occurs due to insufficient validation of the content of upgrade packages. An attacker can upload a malicious archive to the **Upgrade** page of the **Administrative Web Interface** and exploit this vulnerability. A successful exploit can allow the attacker to execute code with *user-level* privileges (the **_nobody** account) on the underlying operating system.
- Mobile and Remote Access (MRA) supports WiFi to LTE handoff and vice-versa on Webex App.

X14.0.2 release

- The Install Wizard can start SSH Service on port 22 (standard SSH port) to set the *root* and *admin* password.
- Alarm to indicate that certificates have expired.

X14.0.1 release

- Multiple Admin Accounts and Groups can have CLI access. For more information, see About the administrator account and field references.
- Two new alarms have been introduced in the trust store and onboarding trust store to notify the administrator.
  - Alarm to indicate that certificate is going to expire in next 21 days.

X14.0 release

- Admins now have the flexibility to configure SSH ciphers on TCP port 22 which is configurable from the web interface, without needing to use CLI commands to update the Expressway SSH configuration.
- To meet Cisco Product Security Baseline, the cipher filters for the following services are updated:
  - SSL ciphers used by Reverse proxy
  - SSL ciphers used by Apache

  - SSL ciphers used by UC Service Discovery
  - SSL ciphers used by XMPP
  - SSL ciphers for LDAP

- To meet Cisco Product Security Baseline, the crypto algorithms of the SSH Key Configuration are updated. Some disallowed key exchange algorithms are removed:
  - ecdh-sha2-nistp521
  - ecdh-sha2-nistp384

  The following key exchange algorithms are added:
  - ecdh-sha2-nistp256
  - diffie-hellman-group14-sha256
  - diffie-hellman-group14-sh1

- Expressway-E is exposed to silent SIP scans (using SIP OPTIONS) and spam calls (using SIP INVITE). This is similar to a DoS attack. To protect from this SIP based DOS attack, SIP Authentication Failure on Fail2Ban is enabled by default for :
  - Fresh Expressway installations from X14.0 and later versions
  - Factory reset with X14.0 or later versions

  But, if you only upgrade SIP-Auth ban it will remain in the same enabled/disabled state as before your upgrade.

- You can configure the Rate Limits for SIP transaction. From the Web UI, you can enable/disable or change number of connections per second and Burst limit values. By default, the connections per second values is 100 and the Burst limit is 20.
- Automated Protection or the SIP Registration failure detection system is now enhanced to cover the following conditions:
  - License limit exceeded
  - Maintenance mode
  - Not permitted by policy
  - Out of resource
  - Registration not allowed

- When an Expressway VM is running on sub-spec hardware with a slow CPU and low memory, an unsupported/non-compliant hardware warning alarm is displayed.
- As part of the enhancements to CUCM/Phone security feature support over MRA, port 6971 is added on the HTTPS allow list for OAuth enabled MRA client to download the configuration file.

(Preview) Hardware Security Module (HSM) Support

From X12.6 release, Expressway supports HSM functionality, on a Preview basis only. HSM safeguards and manages digital keys for strong authentication, and provides crypto-processing for critical functions such as encryption, decryption and authentication for the use of applications, identities, and databases. An HSM device comes as a plug-in card or an external device that attaches directly to your computer or network server. It prevents hardware and software tampering—by raising alarms or by making the HSM inoperable.

A new **Maintenance** > **Security** > **HSM configuration** page is added to the Expressway web user interface.

Expressway currently only supports the nShield Connect XC from Entrust as an HSM provider (on a Preview basis).

Important The “SafeNet Luna” network device from Gemalto is also referenced in the Expressway user interface but, **this device is not currently supported by Expressway**.

(Preview) Headset Capabilities for Cisco Contact Center – MRA Deployments

This feature applies if you deploy Expressway with Mobile and Remote Access. It is currently provided in Preview status only.

New demonstration software now provides some Cisco Contact Center functions on compatible Cisco headsets. From X12.6, Expressway automatically supports these new headset capabilities as a preview feature, if the involved endpoint, headset, and Unified CM are running the necessary software versions. The feature is enabled from the Unified CM interface and you do not need to configure anything on Expressway.

More information is available in the white paper Cisco Headset and Finesse Integration for Contact Center.

(Preview) Push Notifications with Mobile Application Management clients - MRA Deployments

This feature applies if you deploy Expressway with Mobile and Remote Access. It is currently provided in Preview status only.

With this feature, push notification support over Mobile and Remote Access now includes support for Mobile Application Management (MAM) clients like Jabber Intune and Jabber BlackBerry. As a result, the push notification service is available for all devices that are running Jabber Intune and Jabber BlackBerry clients.

(Preview) Push Notifications with Android Devices – MRA Deployments

This feature applies if you deploy Expressway with MRA. In X12.6 it was introduced in Preview status only, due to external product version dependencies.

In X12.6.2, the feature was switched off by default due to a known issue (bug ID CSCvv12541refers).

In X12.7, bug ID CSCvv12541 was fixed. However, this feature remains in Preview status for now, due to pending software dependencies.

How to enable push notifications for Android devices

This feature is enabled through the Expressway command line interface. Only do this **if all IM and Presence Service nodes that service Android users are also running a supported release**.

The CLI command is: *xConfiguration XCP Config FcmService: On*

Note IM and Presence services for users who are currently signed in over MRA will be disrupted when this command is used, so those users will need to sign in again.

(Preview) KEM Support for Compatible Phones - MRA Deployments

We have not officially tested and verified support over MRA for the Key Expansion Module (KEM) accessory for Cisco IP Phone 8800 Series devices. However, we have observed under lab conditions that KEMs with multiple DNs work satisfactorily over MRA. These are **not** official tests, but in view of the COVID-19 crisis, this may be useful information for customers who are willing to use an unsupported preview feature.

SIP path headers must be enabled on Expressway, and you need a Unified CM software version that supports path headers (release 11.5(1)SU4 or later is recommended).

Other Changes in this Release

X14.0.2 release

- **Traffic Server Enforces Certificate Verification**

  Condition -

  Important Before upgrading to X14.0.2 release, make sure the following certificate requirement is met.

  This is due to some improvement in the traffic server service in Expressway.

  Requirement - Add the Certificate Authority (CA) which signed the Expressway-C certificate to the *Tomcat*-trust and *CallManager*-trust list of Cisco Unified Communications Manager (UCM), even if the UCM is in *non-secure* mode. And, restart the following services on CUCM side:

  - Tomcat Service
  - CallManager Service
  - HA Proxy Service (if using TLS on Tomcat)

  Reason - The traffic server service in Expressway sends its certificate whenever a server (UCM) requests it. These requests are for services running on ports other than 8443 (for example, ports 6971, 6972,...). This enforces certificate verification even if UCM is in *non-secure* mode. For more information, see Mobile and Remote Access Through Expressway Deployment Guide.

- Expressway-C supports two new items for UCM on the HTTPS allow list:

  - Create Device
  - Supported Services

- You can configure remote syslog servers and call detail record (CDR) details through a single API. The API has three parts. All the parts can now be set up using REST API.

  Remember This feature is already available in the user interface but incorporating it through an API is easier.

  The following are the main changes.

  1. **Logging options**: You can change Event Log Verbosity to control the granularity of event logging. Toggling to Media Statistics allows you to record call statistics after selecting the method for logging Call Details. It also controls certification-compliant logging for Expressway.

     Configuration Path: `/provisioning/common/logging/options`

  2. **Remote Syslog Servers**: You can specify up to 4 remote syslog servers, with different protocols or log levels, if required. The syslog servers must support BSD or IETF syslog protocols.

     Configuration Path: `/provisioning/common/logging/remotesyslogservers`

  3. **System Metrics Collection**: Select *On* to start collecting system metrics for Expressway.

     Configuration Path: `/provisioning/common/logging/systemmetrics`

X14.0.1 release

- MRA with SSO login in a split VPN situation has been fixed on the Expressway C to keep track of the UCM node used for the login and make sure the same UCM node is used for the messages of login flow which requires the unique CUCM for successful login even if the source IP changes.
- The following MRA Registration issues using a wrong Traversal Zone are fixed.

  1. Adaptive routing support when PRRH “Register” is enabled.
  2. Appropriate Zone lookup and selection when there are 2 zones both for MRA and B2B configured on the same Expressway with PRRH “Register” enabled.

REST API Changes

The REST API for Expressway 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 Expressway.

The API is self-documented using RAML, and you can access the RAML definitions at `https://<ipaddress>/api/raml`.

Table 5: List of REST API(s)

Configuration APIs	API introduced in version
Service Select Wizard	X14.0.3
Ability to acknowledge active Alarms	X14.0.3
Ban/Unban an IP Address	X14.0.3
Exempt an IP Address	X14.0.3
Call Detail Record (CDR) Configuration	X14.0.3
Status - fail2banbannedaddress	X14.0.2
SNMP Configuration	X14.0.1
Alarms - view and acknowledge	X14.0.1
Dedicated Management Interface (DMI)	X12.7
Diagnostic Logging	X12.6.3
Smart Licensing	X12.6
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 X14.0.4
- Issues resolved by X14.0.3
- Issues resolved by X14.0.2
- Issues resolved by X14.0.1
- Issues resolved by X14.0

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.

Note 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**. 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.

From X12.5, Expressway provides limited SIP UPDATE support over MRA connections for session refresh purposes only, as specified by RFC 4028. However, you should not switch this on unless you have a specific requirement to use this capability. Any other use of SIP UPDATE is not supported and features that rely on this method will not work as expected.

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. A list of key unsupported features that we know do not work with MRA is detailed in *Key Supported and Unsupported Features with Mobile and Remote Access* in the Mobile and Remote Access Through Cisco Expressway Guide.

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 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.

Note 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 an VCS-C in each subnet, with an 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.

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

Procedure

Step 1 If you plan to use the log analysis tool, first collect the Cisco VCS logs.

Step 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.

Step 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: 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.

To Reconfigure the MRA Access Control Settings

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.

Before you begin

After the system restarts you need to reconfigure the MRA access control settings.

Procedure

Step 1 On the Cisco VCS Control, go to **Configuration** > **Unified Communications** > **Configuration** > **MRA Access Control**.

Step 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.

Step 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**.

Settings for MRA Access Control

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”. **Note** Do not use it in other cases.	None before MRA turned on UCM/LDAP after MRA turned on

Field	Description	Default
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
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

Field	Description	Default
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

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*.	-

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

MRA Access Control Values Applied by the Upgrade

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 **Note** **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)

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)