Cisco Meeting Server

Cisco Meeting Server Release 2.6.4

Release Notes

December 12, 2019

Contents

What's changed

Version	Change
December 12, 2019	Fourth maintenance release. Beta support for Chromium-based Microsoft Edge browsers See Issues resolved in 2.6.4 Hashes updated.
October 17, 2019	Third maintenance release. Beta support for Yandex browser and new meeting join options introduced. See Issues resolved in 2.6.3 Hashes updated.
October 17, 2019	Issues resolved in 2.6.2 updated. Caution added to upgrade section regarding the need to increase the loadLimit value for load balanced Meeting Server 2000 deployments.
September 5, 2019	Issues resolved in 2.6.0 updated.
August 08, 2019	Second maintenance release. See Issues resolved in 2.6.2 Hashes updated.
May 23, 2019	Issues resolved in 2.6.0 corrected.
May 02, 2019	First maintenance release. See New features introduced in version 2.6.1 See Issues resolved in 2.6.1 Hashes updated.
April 24, 2019	Added requirement to select "Accept Replaces Header" in the SIP Trunk Security Profile on Cisco Unified Communications Manager in order to move a participant between Call Bridges.
April 23, 2019	New release of Cisco Meeting Server software.

1 Introduction

These release notes describe the new features, improvements and changes in release 2.6.4 of the Cisco Meeting Server software.

The Cisco Meeting Server software can be hosted on:

- the Cisco Meeting Server 2000, a UCS 5108 chassis with 8 B200 blades and the Meeting Server software pre-installed as the sole application.
- the Cisco Meeting Server 1000, a Cisco UCS server preconfigured with VMware and the Cisco Meeting Server installed as a VM deployment.
- the Acano X-Series hardware.
- or on a specification-based VM server. Note: From version 2.4, the Meeting Server software no longer supports Microsoft Hyper-V.

Throughout the remainder of these release notes, the Cisco Meeting Server software is referred to as the Meeting Server.

If you are upgrading from a previous version, you are advised to take a configuration backup using the **`backup snapshot <filename>`** command, and save the backup safely on a different device. See the MMP Command Reference document for full details.

Note about certificate validation: From version 2.4, the Web Bridge correctly validates the XMPP Server's TLS certificate. If WebRTC app users have difficulty logging in after you upgrade the Meeting Server, then check that the uploaded XMPP certificate follows the advice in the Certificate Guidelines. Specifically, that the SAN field holds the domain name of the XMPP server. Prior to version 2.4 there were issues in XMPP certificate validation.

Note about Microsoft RTVideo: support for Microsoft RTVideo and consequently Lync 2010 on Windows and Lync 2011 on Mac OS, will be removed in a future version of the Meeting Server software. However, support for Skype for Business and Office 365 will continue.

Note about incoming calls: By default incoming calls are not allowed. To allow incoming calls to Cisco Meeting App users, set parameter **`canReceiveCalls=true`** for API object **`/user/profiles/<user profile id>`**.

Note about chat message board: For existing deployments that use chat message boards, chat will remain enabled when you upgrade to 2.6. Otherwise, you will need to use the API to create a callProfile with parameter **`messageBoardEnabled`** set to true.

1.1 Interoperability with other Cisco products

Interoperability test results for this product are posted to http://www.cisco.com/go/tp-interop, where you can also find interoperability test results for other Cisco conferencing products.

1.2 Cisco Meeting Server platform maintenance

It is important that the platform that the Cisco Meeting Server software runs on is maintained and patched with the latest updates.

1.2.1 Cisco Meeting Server 1000 and other virtualized platforms

The Cisco Meeting Server software runs as a virtualized deployment on the following platforms:

- Cisco Meeting Server 1000
- specification-based VM platforms.

Note: From version 2.4, Cisco Meeting Server software no longer supports Microsoft Hyper-V virtualized deployments.

Note: Although you are encouraged to ensure the virtualized platform running the Cisco Meeting Server software is up to date with the latest patches, only the Cisco Meeting Server 1000 M5 should be upgraded to ESX 6.7 or ESXi 6.5 Update 2. For more information, see here.

1.2.2 Cisco Meeting Server 2000

The Cisco Meeting Server 2000 is based on Cisco UCS technology running Cisco Meeting Server software as a physical deployment, not as a virtualized deployment.

CAUTION: Ensure the platform (UCS chassis and modules managed by UCS Manager) is up to date with the latest patches, follow the instructions in the Cisco UCS Manager Firmware Management Guide. Failure to maintain the platform may compromise the security of your Cisco Meeting Server.

1.3 Interactive API Reference Tool

We recently introduced a new interactive API reference tool enabling you to see a high level view of the API objects and drill down to lower levels for the detail. There are also learning labs to help you get started, these will be added to over time. We encourage you to try out this tool; sometime in the future we will discontinue publishing the pdf version of the API Reference Guide.

https://developer.cisco.com/cisco-meeting-server/

Steps to use the tool:

1. Click **View the docs**

2. Select a category from the list in the left pane. For example: Call Related Methods.

3. Click on any method to see URI: GET/POST/PUT. Refer to the table of parameters and response elements with descriptions. For example: GET https://ciscocms.docs.apiary.io/api/v1/calls?

Note: If you are using a POST/PUT methods, the related 'Attributes' with descriptions appear on the right-hand pane when you select the method.

Learning labs

https://learninglabs.cisco.com/modules/cisco-meeting-server

The learning labs are intended as a starting point, covering a broad cross-section of what is possible with the Cisco Meeting Server API. Every learning lab is a step-by-step tutorial which takes you through the steps to complete the task from start to finish.

Example: The 'Setting up host and guest access with Cisco Meeting Server API' provides instructions to configure ways in which users can join meetings in a space with different options.

1.4 Cisco Meeting App WebRTC Important information

For information on when features are released and bugs fixed for the WebRTC app, refer to the Cisco Meeting App WebRTC Important information guide. All of the information relevant to the WebRTC app has been combined into one document, and is no longer included in the Meeting Server release notes.

The document describes the following:

- Any new or changed feature in the WebRTC app, and details of fixed issues and open issues associated with the WebRTC app with an indication of the version of Meeting Server where this feature/fix is available.
- Any upcoming changes in browsers affecting the WebRTC app, and the affected versions of the app with recommended workarounds.

WebRTC is still an evolving technology and frequent changes are implemented by browser vendors. The Cisco Meeting App WebRTC Important information guide will be updated when we need to inform you of upcoming changes.

1.5 End of Software Maintenance

On release of Cisco Meeting Server software version 2.6, Cisco announces the time line for the end of software maintenance for the software in Table 1.

Table 1: Time line for End of Software Maintenance for versions of Cisco Meeting Server

Cisco Meeting Server software version	End of Software Maintenance notice period
Cisco Meeting Server version 2.4.x	4 months after the first release of Cisco Meeting Server version 2.6. This will be August 22nd 2019.

For more information on Cisco's End of Software Maintenance policy for Cisco Meeting Server click here.

1.6 Using the Cisco Expressway-E as the edge device in Meeting Server deployments

Over the previous few releases of Cisco Expressway software, edge features have been developed to enable the Cisco Expressway-E to be used as the edge device in Meeting Server deployments. Use the TURN server capabilities in Cisco Expressway-E to connect:

- participants using the WebRTC app to conferences hosted on the Meeting Server,
- remote Lync and Skype for Business clients to conferences hosted on the Meeting Server.

In addition, the Cisco Expressway-E can be used as a SIP Registrar to register SIP endpoints or to proxy registrations to the internal call control platform (Cisco Unified Communications Manager or Cisco Expressway-C).

Table 1 below indicates the configuration documentation that covers setting up Cisco Expressway-E to perform these functions. Table 3 below shows the introduction of the features by release.

Note: Cisco Expressway-E can not be used to connect remote Cisco Meeting App thick clients (Windows/Mac desktop or iOS) to conferences hosted on the Meeting Server. Nor can the Cisco Expressway-E be used between on premises Microsoft infrastructure and the Meeting Server. In deployments with on-premises Microsoft infrastructure and the Meeting Server, the Meeting Server must use the Microsoft Edge server to traverse Microsoft calls into and out of the organization.

Note: If you are configuring dual homed conferencing between on-premises Meeting Server and on-premises Microsoft Skype for Business infrastructure, then the Meeting Server automatically uses the TURN services of the Skype for Business Edge.

Table 2: Documentation covering Cisco Expressway as the edge device for the Meeting Server

Edge feature	Configuration covered in this guide
Connect remote WebRTC apps	Cisco Expressway Web Proxy for Cisco Meeting Server Deployment Guide
Connect remote Lync and Skype for Business clients	Cisco Meeting Server with Cisco Expressway Deployment Guide
SIP Registrar or to proxy registrations to the internal call control platform	Cisco Expressway-E and Expressway-C Basic Configuration (X8.11)

Table 3: Expressway edge support for the Meeting Server

Cisco Expressway-E version	Edge feature	Meeting Server version
X8.11	Supported: - load balancing of clustered Meeting Servers, - Microsoft clients on Lync or Skype for Business infrastructure in other organizations, or Skype for Business clients on Office 365 (not "consumer" versions of Skype). - interoperability between on-premise Microsoft infrastructure and on-premise Meeting Server, **where no Microsoft calls traverse into or out of the organization.** - standards based SIP endpoints. - standards based H.323 endpoints. - Cisco Meeting App thin client (Web RTC app) using TCP port 443. Not supported: - off premise Cisco Meeting App thick clients (Windows/Mac desktop or iOS). - interoperability between on-premise Microsoft infrastructure and on-premise Meeting Server **where Microsoft calls traverse into or out of the organization**, in this scenario, the Meeting Server must use the Microsoft Edge server to traverse Microsoft calls into and out of the organization. See Cisco Meeting Server with Cisco Expressway Deployment Guide (2.4/X8.11.4).	2.4

Cisco Expressway-E version	Edge feature	Meeting Server version
X8.10	Supported: - Microsoft clients on Lync or Skype for Business infrastructure in other organizations, or Skype for Business clients on Office 365 (not "consumer" versions of Skype), - standards based SIP endpoints, - Cisco Meeting App thin client (Web RTC app) using UDP port 3478 to connect to the Meeting Server via the Expressway reverse web proxy. Not supported: - load balancing of clustered Meeting Servers, - off premise Cisco Meeting App thick clients (Windows/Mac desktop or iOS) or Cisco Meeting App thin client (Web RTC app) using TCP port 443, - interoperability between on premises Microsoft infrastructure and Meeting Server; in this scenario, the Meeting Server must use the Microsoft Edge server to traverse Microsoft calls into and out of the organization. See Cisco Expressway Web Proxy for Cisco Meeting Server	2.3
X8.9	Supported: - Microsoft clients on Lync or Skype for Business infrastructure in other organizations, or Skype for Business clients on Office 365 (not "consumer" versions of Skype), - standards based SIP endpoints. Not supported: - load balancing of clustered Meeting Servers,, - off-premise Cisco Meeting App thick clients (Windows/Mac desktop or iOS) and Cisco Meeting App thin client (WebRTC app), - interoperability between on premises Microsoft infrastructure and Meeting Server; in this scenario, the Meeting Server must use the Microsoft Edge server to traverse Microsoft calls into and out of the organization See Cisco Expressway Options with Meeting Server and/or Microsoft Infrastructure	2.2

You are encouraged to migrate your Meeting Server deployments from using the Meeting Server edge components to using the Expressway X8.11 (or later) TURN server. The SIP edge, TURN server, internal Firewall and H.323 gateway components will be removed from the Meeting Server software at some point in the future

1.7 Using the Cisco Expressway-C with the Meeting Server in the core network

In addition to deploying Cisco Expressway-E at the edge of the network, Cisco Expressway-C can be deployed in the core network with the Meeting Server. If deployed between the Meeting Server and an on-premises Microsoft Skype for Business infrastructure, the Cisco Expressway-C can provide IM&P and video integration. In addition the Cisco Expressway-C can provide the following functionality:

- a SIP Registrar,
- an H.323 Gatekeeper,
- call control in Meeting Server deployments with Call Bridge groups configured to load balance conferences across Meeting Server nodes.

Table 4:Additional documentation covering Cisco Expressway-C and the Meeting Server

Feature	Configuration covered in this guide
Call control device to load balance clustered Meeting Servers	Cisco Meeting Server 2.4+, Load Balancing Calls Across Cisco Meeting Servers
SIP Registrar	Cisco Expressway-E and Expressway-C Basic Configuration (X8.11)
H.323 Gatekeeper	Cisco Expressway-E and Expressway-C Basic Configuration (X8.11)

Note: When planning the dial plan on Expressway, each Meeting Server in a cluster requires its own neighbour zone on the Cisco Expressway. For more information see Appendix A in the white paper Load Balancing Calls Across Cisco Meeting Servers.

1.7.1 Using the Cisco Expressway H.323 gateway component

In line with Cisco's goal of a single Edge solution across the Cisco Meeting Server and Cisco Expressway, Cisco plans to end of life the Meeting Server H.323 Gateway component. From version 2.4 of the Meeting Server software, there will be no further bug fixes for the H.323 Gateway component. The H.323 component will be removed from the Meeting Server software in a future release. Customers are encouraged to start evaluation of the more mature H.323 Gateway component in the Cisco Expressway, and plan their migration over.

Any H.323 endpoints registered to Expressway-E or Expressway-C will not consume Rich Media Session (RMS) licenses when calling into the Cisco Meeting Server from Expressway version X8.10 onwards.

2 New Features/Changes in version 2.6

Version 2.6 of the Meeting Server software adds the following:

- a change to PMP Plus license usage and changes to license reporting
- support for Skype for Business 2019
- ability to move a participant between conferences
- increase call capacity on Cisco Meeting Server 2000s within Call Bridge Groups
- support for ESXi 6.7 on the Cisco Meeting Server 1000 M5.
- two new features to improve serviceability which will help Cisco Support in diagnosing Meeting Server issues,

In addition:

- ESXi 5.5 and earlier are no longer supported versions of VMware for Cisco Meeting Server.
- dual screen endpoints are enabled by default.
- support for more video streams over distribution links, first previewed in version 2.3, is still a preview feature. The feature creates a more consistent video experience from remote single, dual and three screen end point systems

You are advised not to use beta (or preview) features in a production environment. Only use them in a test environment until they are fully released.

Note: Cisco does not guarantee that a beta (or preview) feature will become a fully supported feature in the future. Beta features are subject to change based on feedback, and functionality may change or be removed in the future.

Note: The term spaces is used throughout the documentation apart from the API guide which still uses the old terminology of coSpaces.

2.1 New features introduced in version 2.6.4

2.1.1 Beta support for Chromium-based Microsoft Edge browser in WebRTC app

Version 2.6.4 adds Beta support for Cisco Meeting App for WebRTC using Chromium-based Microsoft Edge browser on Windows. This is beta quality in current version.

2.2 New features introduced in version 2.6.3

2.2.1 Beta support for Yandex browser in WebRTC app

Version 2.6.3 introduces Beta support for Cisco Meeting App for WebRTC using Yandex browsers on Windows. This is beta quality in current version.

2.2.2 Joining options with no microphone or camera for WebRTC app

Version 2.6.3 introduces some new joining call options.

While joining a meeting, you can now choose 'no camera' or 'no microphone' from the **Joining options** screen. This can be useful if you have a faulty camera or microphone and you can see and hear other participants in the call, but other participants cannot see or hear you.

Note: We do not recommend changing options during a meeting.

To add a camera or a microphone whilst you are in a meeting:

1. Click **Back** to navigate to the main screen. You will still be in the meeting.
2. Click on  to open the **Settings** screen. Select a camera and microphone from the options shown.
3. Click **Return to meeting** to return to the in-meeting screen and continue your meeting with the new options selected.

2.3 New features introduced in version 2.6.1

2.3.1 X-series support

Version 2.6.1 is the first 2.6 release to support X-series.

2.3.2 Additional browser support for WebRTC app

Version 2.6.1 introduces support for Cisco Meeting App for WebRTC using:

- Apple Safari on iOS 12.3
- Apple Safari 12.2 on macOS
- Mozilla Firefox 68

All these browsers are currently in beta (at time of first publication).

See Cisco Meeting App WebRTC Important Information for the latest browser support details.

2.4 License changes

From version 2.6 the following license changes apply.

2.4.1 Change to PMP Plus license usage

From version 2.6, the rules for applying a PMP Plus license have been simplified. Rather than relying on active participation, PMP Plus license consumption will simply follow the space owner. From 2.6, the rules for applying a license are as follows:

When a meeting starts in a space, a Cisco license is assigned to the space. Which license is assigned by the Cisco Meeting Server is determined by the following rules:

- if the space owner is defined and corresponds to a Meeting Server imported LDAP user with an assigned Cisco PMP Plus license, the license of that owner is assigned irrespective of whether the person is active in the conference, if not, then
- if the meeting was created via ad hoc escalation from Cisco Unified Communications Manager, then Cisco Unified Communications Manager provides the GUID of the user escalating the meeting. If that GUID corresponds to a Meeting Server imported LDAP user with an assigned Cisco PMP Plus license, the license of that user is assigned, if not, then
- if the meeting was scheduled via Cisco TMS version 15.6 or newer, then TMS will provide the owner of the meeting. If that user corresponds to a Meeting Server imported LDAP user with an assigned Cisco PMP Plus license, the license of that user is assigned to the meeting, if not then,
- a Cisco SMP Plus license is assigned.

2.4.2 Calculating SMP Plus license usage

For the following specific scenarios, the SMP Plus license consumed for a meeting is reduced to 1/6th of a full SMP Plus license:

- an audio-only conference where no attendees are using video,
- a Lync gateway call unless the Meeting Server is recording or streaming, at which point it is considered a full conference and a full SMP Plus license is consumed,
- a point to point call involving a Cisco Meeting App and a SIP endpoint, or two Cisco Meeting Apps, unless the Meeting Server is recording or streaming, at which point it is considered a full conference and a full SMP Plus license is consumed.

A full SMP Plus license is consumed for any audio-video conference instantiated from a space with the owner property undefined, owned by an imported LDAP user without a PMP Plus license, or owned by an imported LDAP user whose PMP Plus license has already been consumed, this is irrespective of the number of participants.

Note: A point to point call is defined as:

- having no permanent space on the Meeting Server,
- two or less participants, including the recorder or streamer
- no participants hosted on the Lync AVMCU,

This includes Lync Gateway calls as well as other types of calls: point-to-point Cisco Meeting App to Cisco Meeting App, Cisco Meeting App to SIP and SIP to SIP.

2.4.3 License reporting

From version 2.6, the Meeting Server records license usage for each license type and reports the usage over a 90 day window to Cisco Meeting Management.The usage of recording licenses indicates the number of conferences recording concurrently, similarly the streaming license usage indicates the number of conferences streaming concurrently. For more information refer to the Cisco Meeting Management 2.6 Release Notes.

2.5 Skype for Business 2019

From version 2.6, the Meeting Server supports Skype for Business 2019. The same deployment restrictions apply to Meeting Server deployments with Skype for Business 2019 as previous versions of Skype and Lync. These are:

- Cisco Expressway-E cannot be used between on-premises Microsoft infrastructure and the Meeting Server. In deployments with on premises Microsoft infrastructure and the Meeting Server, the Meeting Server must use the Microsoft Edge server to traverse Microsoft calls into and out of the organization.
- If you are configuring dual homed conferencing between on-premises Meeting Server and on-premises Microsoft Skype for Business infrastructure, then the Meeting Server automatically uses the TURN services of the Skype for Business Edge.

2.6 Moving a participant between conferences

From version 2.6, a participant using a SIP endpoint registered to Cisco Unified Communications Manager can be moved between meetings hosted on Meeting Servers. This allows conference organizers to use previously created spaces for breakout sessions, splitting a large group into smaller groups to encourage collaboration, or to screen participants before being allowed into a meeting.

A participant can be moved between any type of call with the exception of moving to dual homed conferences. For instance, a participant can be moved between meetings associated with a space, and meetings with a call forwarding rule applied. A SIP participant which supports SIP replaces can be moved from a conference hosted on an AVMCU. Currently, there is also a limitation on moving a participant within an Ad hoc call, see below.

Moving a participant between conferences on different Call Bridges requires each trunk between Cisco Unified Communications Manager and a Call Bridge to be configured to use a

SIP Trunk Security Profile that has the "Accept Replaces Header" check box selected, this is required even if load balancing is not configured within the deployment. For more information on the SIP Trunk Security Profile, see the Security Guide for Cisco Unified Communications Manager.

Note: SIP calls with Cisco Expressway/VCS or Cisco Meeting App calls are not supported by the move participant feature.

Use either Cisco Meeting Management or the Meeting Server API to move a participant. This section covers using the Meeting Server API, refer to the Cisco Meeting Management 2.6 Release Notes for information on how to move a participant between meetings using Cisco Meeting Management. There is no facility to move participants in bulk using the API.

The source and destination meetings can be hosted on the same Call Bridge or on different Call Bridges within a cluster. For a participant to be moved to a different conference, the Call Bridge that you send the API request to must be aware of the ID of the target conference. The participant ID does not have to correspond to a participant existing on that Call Bridge, the Call Bridge will query other Call Bridges in the cluster in an attempt to find the participant.

Note: When a participant is moved to a new conference, the participant is given a new participant ID. During the move there is a period where both the old and new participant IDs exist while the callLeg is being transferred. The callLeg ID also changes during the move.

To move a participant to a different conference, a new **`movedParticipant`** parameter has been added to **`calls/<call id>/participants`**. POST to object **`/calls/<call id>/participants`** the parameter **`movedParticipant`** with the ID of the participant to move. Refer here for an example of the steps involved.

2.6.1 Specifying callBridge and callBridgeGroups when moving a participant

When moving a participant between conferences, do not specify the **`callBridge`** or **`callBridgeGroup`** API parameters, in the POST to **`calls/<call id>/participants`**, the parameters will be ignored if specified. Instead, the participant will be placed automatically; they will remain within the same Call Bridge group providing both **`loadBalancingEnabled`** and **`loadBalanceOutgoingCalls`** are set to **`true`** for that Call Bridge group, otherwise the participant will remain homed on the same Call Bridge in the cluster. When moving a remote participant between conferences homed on different Call Bridges, a peer link between the Call Bridges will be created for the participant.

2.6.2 Configuration settings for a participant being moved

Moving a participant between conferences will not move any configuration settings associated with the participant, they will have the same configuration as if they had dialed into the destination conference themselves. However, it is possible to override specific settings for the

participant as part of the POST to **/calls/<call id>/participants**. For example: you might want to ensure that the participant had the same importance value in the destination conference as they have in the conference they are moving from, in which case set **movedParticipant** with the ID of the participant to be moved and **importance** set to the same value as was set for the conference they are moving from.

2.6.3 Limitations when moving a participant

The following lists the limitations which must be considered when planning to move a participant:

- a Cisco Meeting App user cannot currently be moved between conferences.
- If a participant is moved while sharing content, they may continue to share content in the new meeting.
- Move participant currently allows a SIP endpoint to be dialed out to the AVMCU, but fails to initiate and connect the corresponding Lync-side call legs. You are advised to avoid moving a participant using a SIP endpoint to a dual homed call, as they will only see video from participants homed to the Meeting Servers, and will not see Lync or Skype for Business clients.
- A participant cannot be moved between conferences if the outbound call is routed through a Cisco Expressway.
- Cisco Unified Communications Manager is not aware of participants moving within an escalated Ad hoc call. If three participants join an Ad hoc call with two of them being dialed out via moveParticipant, if one of these participants drop from the call, the call will change to a point to point call.

2.6.4 Checking that participants have moved

When moving a participant between conferences, there is no provision in the API to check that the move has been successful. Instead use CDRs and Events to track the progress of the move participant.

From 2.6, the **callLegStart** CDR contains additional parameters to indicate:

- whether the participant owning this call leg can be moved,
- the ID of the original call leg that the participant was moved from,
- the ID of the Call Bridge hosting the conference that the moved participant's call leg was originally homed on.

In addition, the event resource **callRoster** includes additional parameters to indicate:

- whether the participant can be moved,
- the original participant ID,

- the ID of the Call Bridge hosting the conference that this participant was moved from.

2.7 Cisco Meeting Server 2000 call capacity in Call Bridge Groups

In version 2.4, the HD/FullHD call capacities of the Cisco Meeting Server 2000 platform were increased but the new capacity was not supported in Call Bridge Groups and load balancing, see Table 6. From version 2.6 the load limit logic for the Cisco Meeting Server 2000 platform has been updated and the call capacities listed in Table 5 below are now deployable with Call Bridge Groups, Call Bridge clustering, and load balancing.

From version 2.6, the **`loadlimit`** for the Cisco Meeting Server 2000 platform has increased from 500000 to 700000 and the load calculation for the different call resolutions has been updated to match the new 700000 limit. Load limits for other Meeting Server platforms stay as they were previously; these changes only apply to the Cisco Meeting Server 2000.

Note: Existing Cisco Meeting Server 2000 deployments that are using load limits and load balancing must manually update their **`loadLimit`** values after upgrading to version 2.6, both to utilize this new feature and to avoid a capacity decrease for SD calls.

Table 5: Call capacity on Cisco Meeting Server 2000 from version 2.6

Type of call	Call capacity from version 2.6 for Cisco Meeting Server 2000 (single, clustered or within a Call Bridge Group)
Full HD (1080p30)	350
HD (720p30)	700
SD (448p30)	1000
Audio	3000

Table 6: Call capacity on Cisco Meeting Server 2000 for versions 2.4 and 2.5

Type of call	Call capacity on a single Cisco Meeting Server 2000 or clustered servers, versions 2.4 and 2.5	Call capacity on a Cisco Meeting Server 2000 within a Call Bridge Group, versions 2.4 and 2.5
Full HD (1080p30)	350	250
HD (720p30)	700	500
SD (448p30)	1000	1000
Audio	3000	3000

Note: The capacities in the above tables are approximations based on computational load, and actual capacity will vary with real-time factors such as dynamic resolutions, number of streams and content sharing. Call counts also include non-participant call legs such as distribution links, recorder/clients, and gateway call legs. Load limits provide the means to cap total utilization across all these factors on a single Meeting Server instance rather than on a limited participant count metric.

Note: The participant limit per conference per server across all Meeting Server platforms remains at 450, the number of participants per conference across distributed servers remains at 2600.

2.8 ESXi support

Version 2.6 adds support for ESXi 6.7 Update 1 (or later) on the Cisco Meeting Server 1000 M5. ESXi 6.7 requires virtual hardware vsm-14.

ESXi 5.5 and earlier are no longer supported for use with Cisco Meeting Server.

Note: Due to changes in VMware, we do not recommend upgrading to ESXi 6.7 or ESXi 6.5 Update 2 for Cisco Meeting Server 1000 M4, or spec based VMs. This is due to significant packet loss being observed when a Cisco Meeting Server 1000 M4, upgraded to ESXi 6.7, operates under high load. Cisco Meeting Server 1000 M5 are unaffected by the VMware change.

2.9 New serviceability feature

Two new serviceability features are introduced in version 2.6, these will help Cisco Support in diagnosing Meeting Server issues. The improvement includes:

- the timestamps shown in syslogs and the Web Admin now show milliseconds to facilitate interpreting packet captures. Note that there may be a few millisecond difference in the time stamp shown in the Web Admin compared to the syslog.
- further improvements to more easily determine which log messages are applicable to a conference.

Neither of these serviceability features are intended for use by customers, however Cisco Support may request syslogs from a customer, and will use these new features to determine any issues.

2.10 Summary of MMP changes

There are no new additions or changes to the MMP commands for version 2.6.4.

2.11 Summary of API Additions & Changes

New API functionality for the Meeting Server 2.6 includes:

- new API objects to enable an administrator to retrieve license usage from the Meeting Server,
- new API parameters to enable an administrator to move a participant between conferences,

In addition, support for dual screen endpoints is enabled by default in version 2.6. Cisco Meeting Server release notes for version 2.3 incorrectly stated that support for dual screen endpoints was enabled by default (**sipMultistream=true**). However the default setting for **sipMultistream** was set to false in versions 2.3, 2.4 and 2.5.

2.11.1 Retrieving license usage snapshots from a Meeting Server

Use GET on **/system/MPLicenseUsage/knownHosts** to retrieve host ids of the Meeting Servers in the deployment. Supply an offset and limit if required to retrieve host ids other than those on the first page of the list.

Use GET on **/system/MPLicenseUsage** to retrieve license usage from the Call Bridge of the Meeting Server with the specified host id. Supply a start and end time for the snapshot. Provides information on number of personal licenses in use, number of shared licenses in use which are audio only, point to point, or neither audio or point to point, number of calls being recorded and number of streamed calls.

Note: personal and shared licenses are normalized over the number of Call Bridges that the call spans.

2.11.2 Moving a participant between conferences

To determine whether a participant can be moved to a different conference on the same Call Bridge or a different Call Bridge in the cluster, use GET on either **/participants/<participant id>** or **/callLegs/<call leg id>**:

- Use GET on **/participants/<participant id>** to return the setting for **canMove**, if set to "true" the participant can be moved, if set to "false" the participant cannot be moved.
- Use GET on **/callLegs/<call leg id>** to return the setting for **canMove**, if set to "true" the participant owning the call leg can be moved, if set to "false" the participant owning the call leg cannot be moved.

To move a participant to a different conference, a new **movedParticipant** parameter has been added to **/calls/<call id>/participants**:

- POST to **/calls/<call id>/participants** the new **movedParticipant** with the ID of the participant to be moved, where **<call id>** is the ID of the target conference. Note: the

original Call Bridge or Call Bridge Group will be used, and any Call Bridge or Call Bridge Group parameters specified in the POST will be ignored.

After moving a participant to a different conference:

- To determine the call leg that the participant was moved from, use GET on **/participants/<participant id>**. A new response value of **movedCallLeg** will be returned with the ID of the original call leg before the participant was moved.
- To find the Call Bridge that homed the call leg that the participant was moved from, use GET on **/participants/<participant id>**. A new response value of **movedCallLegCallBridge** will be returned with the ID of the Call Bridge that homed the original call leg before the participant was moved.
- To determine if the specified call leg was created as a result of moving a participant to a new conference, use GET on **/callLegs/<call leg id>**. A new response value of **movedCallLeg** will be returned with the ID of the original call leg before the participant was moved, and a new response value of **movedCallLegCallBridge** will be returned with the ID of the Call Bridge that homed the original call leg before the participant was moved.

Note: Even if the API request succeeds, the move participant may not succeed if the SIP replaced call out for the new participant fails. If this happens then the new participant will be destroyed and the participant that was due to be replaced will remain in the call. The status of the new and replaced participants will be relayed via CDRs and events messages.

Example

To move a participant between conferences:

1. Identify the ID of the participant to be moved from the conference specified by **<call id>**

   GET **/calls/<call id>/participants**
2. Determine whether the identified participant can be moved using the ID of the participant

   GET **/participants/<participant id>**

   the participant can be moved if response value **canMove** is set to **true**.
3. Move the identified participant to the destination conference with the ID specified by **<call id>**

   POST to object **/calls/<call id>/participants** the parameter **movedParticipant** with the ID of the participant to move.

   Note: The ID of the participant to be moved will be destroyed and replaced with a new ID as part of the move. The callLeg ID also changes during the move.

Responses

HTTP response	Description
200 OK, with GUID of the new participant given inside the Location: header	Move participant successful, but see note below table.
400 error with the following data: `<?xml version="1.0"?><failureDetails><parameterError parameter="remoteParty or movedParticipant" error="mandatory" /></failureDetails>`	Move failed because neither **remoteParty** or **movedParticipant** was provided
400 error with the following data: `<?xml version="1.0"?><failureDetails><parameterError parameter="movedParticipant" error="invalidValue" /></failureDetails>`	Move failed because the **movedParticipant** GUID was malformed
400 error with the following data: `<?xml version="1.0"?><failureDetails><participantDoesNotExist /></failureDetails>`	Move failed because the **movedParticipant** GUID did not correspond to a participant hosted on a Call Bridge in the cluster
400 error with the following data: `<?xml version="1.0"?><failureDetails><participantCannotBeMoved /></failureDetails>`	Move failed because the **movedParticipant** GUID did not correspond to a participant that supports being moved

2.11.3 Support for dual screen endpoints enabled by default

From version 2.6, support for dual screen endpoints is enabled by default. This feature allows video to be shown across both screens of a dual screen endpoint running CE9.1.4 (or later) that are in local calls within your network or for calls over Cisco Expressway X8.9 (or later).

Note: Prior to version 2.6, the feature was disabled by default.

When content is being shared with a dual screen endpoint, either one video and one content stream is sent, or in the case of a dual screen endpoint with a 3rd monitor connected, two video streams and one content stream are sent. For more information on this feature see this FAQ.

Disabling dual screen endpoint support

To disable dual screen endpoint support:

1. Identify the compatibilityProfile that is applied to **/system/profiles** with **sipMultistream** set to true.

2. PUT to /compatibilityProfiles/<compatibility profile id> the parameter **sipMultistream** set to false, where **<compatibility profile id>** is the ID of the compatibilityProfile identified in step 1.

For more information on the API, see the Cisco Meeting Server 2.6 API reference Guide.

2.12 Summary of CDR Changes

Version 2.6 has the following addition to the Call Detail Records of the Meeting Server.

- New parameters of **canMove**, **movedCallLeg** and **movedCallLegCallBridge** in the **callLegStart** record.

Table 7: Additional parameters in **callLegStart** record

Parameter	Type	Description
canMove	true|false	Indicates whether the participant owning this call leg can be moved using the movedParticipant API command.
movedCallLeg	ID	If this call leg was created as part of a participant move, the ID is the GUID of that participant's call leg that it was moved from.
movedCallLegCallBridge	ID	If this call leg was created as part of a participant move, the ID is the GUID of the Call Bridge hosting the conference that the moved participant's call leg was homed on.

2.13 Summary of Event Changes

Version 2.6 has the following addition to subscribable events on the Meeting Server:

- New parameters of **canMove**, **movedParticipant** and **movedParticipantCallBridge** in the **callRoster** event resource.

Table 8: Additional parameters in **callRoster** event resource

Parameter	Type	Description
canMove	true|false	Indicates whether this participant can be moved using the movedParticipant API command.
movedParticipant	ID	If this participant was created as part of a participant move, the ID is the GUID of the participant that this participant was moved from.
movedParticipantCallBridge	ID	If this participant was created as part of a participant move, the ID is the GUID of the Call Bridge hosting the conference that this participant was moved from.

3 Upgrading, downgrading and deploying Cisco Meeting Server software version 2.6

This section assumes that you are upgrading from Cisco Meeting Server software version 2.5. If you are upgrading from an earlier version, then Cisco recommends that you upgrade to 2.5 first following the instructions in the 2.5.x release notes, before following any instructions in these Cisco Meeting Server 2.6 Release Notes. This is particularly important if you have a Cisco Expressway connected to the Meeting Server.

Note: Cisco has not tested upgrading from a software release earlier than 2.5.

To check which version of Cisco Meeting Server software is installed on a Cisco Meeting Server 2000, Cisco Meeting Server 1000, or previously configured VM deployment, use the MMP command **`version`**.

If you are configuring a VM for the first time then follow the instructions in the Cisco Meeting Server Installation Guide for Virtualized Deployments.

3.1 Upgrading to Release 2.6

The instructions in this section apply to Meeting Server deployments which are not clustered. For deployments with clustered databases read the instructions in this FAQ, before upgrading clustered servers.

CAUTION: Before upgrading or downgrading Meeting Server you must take a configuration backup using the **`backup snapshot <filename>`** command and save the backup file safely on a different device. See the MMP Command Reference document for full details. Do **not** rely on the automatic backup file generated by the upgrade/downgrade process as it may be inaccessible in the event of a failed upgrade/downgrade.

Upgrading the firmware is a two-stage process: first, upload the upgraded firmware image; then issue the upgrade command. This restarts the server: the restart process interrupts all active calls running on the server; therefore, this stage should be done at a suitable time so as not to impact users, or users should be warned in advance.

CAUTION: When upgrading Meeting Server 2000 from 2.5 (or earlier) to 2.6 (or later), you need to increase the loadLimit value for load balanced Meeting Server 2000 deployments to ensure maximum capacity.

For each Meeting Server 2000 being upgraded, change the **`loadLimit`** field in **`system/configuration/cluster`** API:

- from 500,000 (suitable for 2.5 and earlier)
- to 700,000 (suitable for 2.6 and later)

This change is required to benefit from the increased capacity in HD/fullHD explained in Section 2.7. If this configuration change is not done, it will result in a capacity decrease for SD calls in load balancing deployments.

To install the latest firmware on the server follow these steps:

1. Obtain the appropriate upgrade file from the software download pages of the Cisco website:

   Cisco_Meeting_Server_2_6_4_CMS2000.zip

   This file requires unzipping to a single upgrade.img file before uploading to the server. Use this file to upgrade Cisco Meeting Server 2000 servers.

   Hash (SHA-256) for upgrade.img file:
   7496316306981ce86e20810624a45f2bec7264a6478702e517ef3738d592d8f9

   Cisco_Meeting_Server_2_6_4_vm-upgrade.zip

   This file requires unzipping to a single upgrade.img file before uploading to the server. Use this file to upgrade a Cisco Meeting Server virtual machine deployment.

   Hash (SHA-256) for upgrade.img file:
   e8acffe74b48ff82297e3f504f4a65daf311b8337d6976e5509dbe4ab3fddcec

   Cisco_Meeting_Server_2_6_4_x-series.zip

   This file requires unzipping to a single upgrade.img file before uploading to the server. Use this file to upgrade Acano X-series servers.

   Hash (SHA-256) for upgrade.img file:
   ad69b77728c1ac9b2fd0b589dd3c135420180e387573af2c381489e66f062afd

   Cisco_Meeting_Server_2_6_4.ova

   Use this file to deploy a new virtual machine via VMware.

   For vSphere6, hash (SHA-512) for Cisco_Meeting_Server_2_6_3_vSphere-6_0.ova file:
   5fc6821a1a1bcbb6cc4aa3e996269a445528abaf449db596db794a7faabc0d23fd390c14fd134092740bb7925c0feda28da455deb559410dfc866b9af6b0b1ff

   For vSphere6.5 and higher, hash (SHA-512) for Cisco_Meeting_Server_2_6_3_vSphere-6_5.ova file:
   8683e77c3f470307e45295403248db1ecdd1838c890d77218b9927c0a4e4e6dc23d2dcfce7bfbc8f935dd915df6f091b3daa7ccd81f5ef1bd2bb8856ffebe989

2. To validate the OVA file, the checksum for the 2.6.4 release is shown in a pop up box that appears when you hover over the description for the download. In addition, you can check the integrity of the download using the SHA-512 hash value listed above.

3. Using an SFTP client, log into the MMP using its IP address. The login credentials will be the ones set for the MMP admin account. If you are using Windows, we recommend using the WinSCP tool.

   Note: If you are using WinSCP for the file transfer, ensure that the Transfer Settings option is 'binary' not 'text'. Using the incorrect setting results in the transferred file being slightly smaller than the original and this prevents successful upgrade.

   Note:
   a) You can find the IP address of the MMP's interface with the **`iface a`** MMP command.
   b) The SFTP server runs on the standard port, 22.

4. Copy the software to the Server/ virtualized server.
5. To validate the upgrade file, issue the **`upgrade list`** command.
   a. Establish an SSH connection to the MMP and log in.
   b. Output the available upgrade images and their checksums by executing the upgrade list command.

      `upgrade list`
   c. Check that this checksum matches the checksum shown above.
6. To apply the upgrade, use the SSH connection to the MMP from the previous step and initiate the upgrade by executing the **`upgrade`** command.
   a. Initiate the upgrade by executing the upgrade command.
      `upgrade`
   b. The Server/ virtualized server restarts automatically: allow 10 minutes for the process to complete.
7. Verify that the Meeting Server is running the upgraded image by re-establishing the SSH connection to the MMP and typing:
   `version`
8. Update the customization archive file when available.
9. If you are deploying a scaled or resilient deployment read the Scalability & Resilience Deployment Guide and plan the rest of your deployment order and configuration.
10. If you have deployed a database cluster, be sure to run the **`database cluster upgrade_schema`** command after upgrading. For instructions on upgrading the database schema refer to the Scalability & Resilience Deployment Guide.
11. You have completed the upgrade.

3.2 Downgrading

If anything unexpected occurs during or after the upgrade process you can return to the previous version of the Meeting Server software. Use the regular upgrade procedure to "downgrade" the Meeting Server to the required version using the MMP **`upgrade`** command.

1. Copy the software to the Server/virtualized server.
2. To apply the downgrade, use the SSH connection to the MMP and start the downgrade by executing the **`upgrade <filename>`** command.

   The Server/virtualized server will restart automatically – allow 10-12 minutes for the process to complete and for the Web Admin to be available after downgrading the server.
3. Log in to the Web Admin and go to **Status > General** and verify the new version is showing under **System status**.
4. Use the MMP command **`factory_reset app`** on the server and wait for it to reboot from the factory reset.
5. Restore the configuration backup for the older version, using the MMP command **`backup rollback <name>`** command.

   Note: The **`backup rollback`** command overwrites the existing configuration as well as the license.dat file and all certificates and private keys on the system, and reboots the Meeting Server. Therefore it should be used with caution. Make sure you copy your existing cms.lic file and certificates beforehand because they will be overwritten during the backup rollback process. The .JSON file will not be overwritten and does not need to be re-uploaded.

   The Meeting Server will reboot to apply the backup file.

   For a clustered deployment, repeat steps 1-5 for each node in the cluster.
6. In the case of XMPP clustering, you need to re-cluster XMPP:
   a. Pick one node as the XMPP master, initialize XMPP on this node
   b. Once the XMPP master has been enabled, joining any other XMPP nodes to it
   c. Providing you restore using the backup file that was created from the same server, the XMPP license files and certificates will match and continue to function
7. Finally, check that:
   - the Web Admin interface on each Call Bridge can display the list of coSpaces
   - dial plans are intact
   - XMPP service is connected
   - no fault conditions are reported on the Web Admin and log files

- you can connect using SIP and Cisco Meeting Apps (as well as Web Bridge if that is supported)

The downgrade of your Meeting Server deployment is now complete.

3.3 Cisco Meeting Server 2.6 Deployments

To simplify explaining how to deploy the Meeting Server, deployments are described in terms of three models: the single combined Meeting Server, the single split Meeting Server and the deployment for scalability and resilience. All three different models may well be used in different parts of a production network.

3.3.1 Deployments using a single host server

If you are deploying the Meeting Server as a single host server (a "combined" deployment), we recommend that you read and follow the documentation in the following order:

1. Appropriate Installation Guide for your Cisco Meeting Server (Cisco Meeting Server 2000, Cisco Meeting Server 1000 and virtualized deployments, or the installation guide for Acano X-Series Server).
2. The Single Combined Meeting Server Deployment Guide enabling all the solution components on the single host. This guide refers to the Certificate Guidelines for Single Combined Server Deployments for details on obtaining and installing certificates for this deployment.

Note: The Cisco Meeting Server 2000 only has the Call Bridge, Web Bridge, XMPP server and database components. It can be deployed as a single server on an internal network, but if a deployment requires firewall traversal support for external Cisco Meeting App clients, then TURN server and Load Balancer edge components need to be deployed on a separate Cisco Meeting Server 1000 or specification-based VM server - see the" single split" deployment below.

3.3.2 Deployments using a single split server hosted on a Core server and an Edge server

If you are deploying the Meeting Server in a split server model, we recommend that you deploy the XMPP server on the Core server, and deploy the Load Balancer on the Edge server.

Read and follow the documentation in the following order:

1. Appropriate Installation Guide for your Cisco Meeting Server
2. The Single Split Meeting Server Deployment Guide. This guide refers to the Certificate Guidelines for Single Split Server Deployments for details on obtaining and installing certificates for this deployment.

3.3.3 Deployments for scalability and resilience

If you are installing the Meeting Server for scalability and resilience using multiple host servers, we recommend that you deploy the XMPP server on Core servers, and deploy Load Balancers on the Edge server.

Read and follow the documentation in the following order:

1. Appropriate Installation Guide for your Cisco Meeting Server
2. The Scalability and Resilience Deployment Guide. This guide refers to the Certificate Guidelines for Scalable and Resilient Server Deployments for details on obtaining and installing certificates for this deployment.

4 Bug search tool, resolved and open issues

You can now use the Cisco Bug Search Tool to find information on open and resolved issues for the Cisco Meeting Server, 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.

1. Using a web browser, go to the Bug Search Tool.
2. Sign in with a cisco.com registered username and password.

To look for information about a specific problem mentioned in this document:

1. 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**

   or,

   in the **Product** field select **Series/Model** and start typing `Cisco Meeting Server`, then in the **Releases** field select **Fixed in these Releases** and type the releases to search for example `2.6.4`.
2. From the list of bugs that appears, filter the list using the *Modified Date*, *Status*, *Severity*, *Rating* drop down lists.

The Bug Search Tool help pages have further information on using the Bug Search Tool.

4.1 Resolved issues

Issues seen in previous versions that are fixed in 2.6.4

Cisco identifier	Summary
CSCvs23685	In certain circumstances Meeting App users are disconnected and deinstatiated. Typically this can occur if many long names are entered with non-standard Latin characters resulting in the names becoming even longer due to the way the non-standard characters are encoded.
CSCvr86934	In some scenarios, if the recording is started before a peer link call, that recording may intermittently stop after peer link is received from the remote Call Bridge.
CSCvr80166	Auto recording fails to start in a meeting scheduled by TMS where TMS makes endpoints dial into different Call Bridges to join the same meeting.
CSCvr13451	The Streamer disconnects and reconnects under packet loss conditions.

Cisco identifier	Summary
CSCvr71743	When participantLimit is set in tenant level, a streaming or recording session is counted as a participant. This reduces the number of actual participants who can join meetings.
CSCvq93115	A Skype for Business client is not able to unmute their endpoint for the first time when the endpoint joins a default-muted AVMCU meeting via Meeting Server. It starts working from the second unmute and thereafter.
CSCvq45298	On a webRTC/Meeting App point-to-point call where each of the calls is hosted on a separate Call Bridge, the peer link that connects them intermittently terminates resulting in call disconnection.
CSCvk65529	On rare occasions Cisco Meeting Server may unexpectedly restart with the following message: sf_assert failed server/media/startup/server_media_xccp_handler.cpp:767

Issues seen in previous versions that are fixed in 2.6.3

Cisco identifier	Summary
CSCvq88442	In a clustered environment, when applying rxVideoMute=true to "/calls/<call id>/participants/*" the video in all peer nodes is frozen.
CSCvq84608	A splash screen momentarily displays (< 1 second) on the upper left video pane when a participant joins a conference. This occurs so quickly that the newly joined participant may not notice it.
CSCvq64378	On Cisco Meeting Server the Call Bridge up time is being reset silently. This doesn't affect normal operations.
CSCvo80460	Occasionally a SIP call is dropped by the far end due to an INVITE timeout.

Issues seen in previous versions that are fixed in 2.6.2

Cisco identifier	Summary
CSCvp89189	In a deployment of multiple XMPP servers, recording may intermittently fail when one of the XMPP servers is turned off.
CSCvq33598	Meeting Server goes into a reboot cycle after upgrade from version 2.5.1 to 2.6.1 if hexadecimal DSCP values are configured.
CSCvq30379	Calls into a conference featuring no other local participants do not result in distribution links being created to other call bridges that do have active participants for the conference in other regions.
CSCvp96569	In rare circumstances, a participant's content stream may not be seen by other conference participants after content is restarted.

Cisco identifier	Summary
CSCvp96694	In rare circumstances, temporary poor video quality may be seen on immersive systems connected to a Meeting Server under conditions of high load.
CSCvp30756	On Meeting Server 2000, Webbridge redirect is not working. The MMP command **`webbridge url-redirect <url>`** has no effect.
CSCvp06073	When a presentation is shared from WebRTC when using the 'Management and Presentation' joining method, the negotiated bandwidth for the presentation stream is capped which leads to poor quality being seen by the receivers.
CSCvp43740	DTMF tones from three screen systems may not be recognized correctly by the Meeting Server. These systems may be unable to navigate a Meeting Server IVR or enter a passcode for a meeting.
CSCvq72054 and CSCvo75687	Unexpected media module restart may occur when receiving Skype for Business content share.
CSCvo91844	Degraded audio may occur on a fully loaded Meeting Server with many audio participants.
CSCvo10678	In a distributed call with recording started, whenever the distributed call is dropped, the recording/streaming is stopped, even though there are participants remaining in the conference.
CSCvp64154	Occasionally the peer link call leg does not present and so participants hosted on different Call bridges in a cluster cannot see and hear each other.

Issues seen in previous versions that are fixed in 2.6.1

Cisco identifier	Summary
CSCvp29391	WebRTC calls on Meeting Server using Apple Safari will not work after updating to Apple Safari on iOS 12.3 or later, and Apple Safari 12.2 on macOS and later.
CSCvp37201	WebRTC calls on Meeting Server using Mozilla Firefox will not work after updating to version 68.
CSCvp38323	Frozen video seen on some Skype for Business participants when Meeting Server sends dual video streams to an AVMCU conference.
CSCvo82633	Occasionally the Recorder does not record for SIP calls when the CallProfile is set to Automatic
CSCvk22499	In rare circumstances, Meeting Server's Callbridge component may restart unexpectedly when a participant joins a meeting.

Note: Refer to the Cisco Meeting App WebRTC Important information guide for information on resolved issues that affected the WebRTC app.

Issues seen in previous versions that are fixed in Cisco Meeting Server 2.6.0 software.

Cisco identifier	Summary
CSCvr16426	The "Participant add" ActiveControl option can be seen on ActiveControl-compatible endpoints that are members of a Dual Home meeting, even though the function is not supported and will not work correctly. From 2.6 onwards, the "Participant add" ActiveControl option is no longer advertised to endpoints in Dual Home meetings.
CSCvp38354	In rare circumstances, the Call Bridge on the Cisco Meeting Server 2000 may restart unexpectedly when under heavy load.
CSCvn52404	In a dual homed conference with only two participants, one SIP and one Skype client, the DTMF profile is not applied. For example, if the Skype client mutes the SIP endpoint then the SIP endpoint can not unmute itself using DTMF.
CSCvm65675	The Call Bridge does not decode video properly from a peer link call leg when using Cisco Unified Communications Manager as the call control device.

4.2 Open issues

Note: Refer to the Cisco Meeting App WebRTC Important information guide for information on open issues affecting the WebRTC app.

The following are known issues in this release of the Cisco Meeting Server software. If you require more details enter the Cisco identifier into the Search field of the Bug Search Tool.

Cisco identifier	Summary
CSCvp34817	In a Cisco Expressway deployment, a participant's display name is not retained when moving a participant between meetings, this affects the display name returned in the Web Admin interface, API, CDR records etc. In addition, when the participant's call leg is load balanced across Meeting Server, the participant's display name will not display correctly in apps (for example Cisco Meeting Management) that use CDRs to determine the participant's display name.
CSCvn65112	For locally hosted branding, if the audio prompt files are omitted then the default built-in prompts are used instead. To suppress all audio prompts use a zero-byte file, rather than no file at all.
CSCvm56734	In a dual homed conference, the video does not restart after the attendee unmutes the video.
CSCvj49594	ActiveControl does not work after a hold/resume when a call traverses Cisco Unified Communications Manager and Cisco Expressway.
CSCvh23039	The Uploader component does not work on tenanted recordings held on the NFS.

Cisco identifier	Summary
CSCvh23036	DTLS1.2, which is the default DTLS setting for Meeting Server 2.4, is not supported by Cisco endpoints running CE 9.1.x. ActiveControl will only be established between Meeting Server 2.4 and the endpoints, if DTLS is changed to 1.1 using the MMP command `tls-min-dtls-version 1.0`.
CSCvh23028	Changing the interface that the Web Bridge listens on or receiving a DHCP lease expire, will cause the Web Bridge to restart. WebRTC App users may have to log in again.
CSCvg62497	If the NFS is set or becomes Read Only, then the Uploader component will continuously upload the same video recording to Vbrick. This is a result of the Uploader being unable to mark the file as upload complete. To avoid this, ensure that the NFS has read/write access.
CSCve64225	Cisco UCS Manager for Cisco Meeting Server 2000 should be updated to 3.1(3a) to fix OpenSSL CVE issues.
CSCve37087 but related to CSCvd91302	One of the media blades of the Cisco Meeting Server 2000 occasionally fails to boot correctly. Workaround: Reboot the Fabric Interconnect modules.

In addition there is the following limitation:

CAUTION: The maximum number of concurrent XMPP clients supported by the current Meeting Server software is 500.This maximum is a total number of all different clients (Cisco Meeting App, WebRTC Sign-in and WebRTC Guest clients) registered at the same time to clustered Meeting Servers. If the number of concurrent XMPP registrations exceeds 500 sessions, some unexpected problems with sign in may occur or it may lead to a situation where all currently registered users need to re-sign in, this can cause a denial of service when all users try to sign in at the same time.

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 of this document are considered uncontrolled. See the current online version for the latest version.

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

Cisco Trademark