Cisco Meeting Server

Cisco Meeting Server Release 2.8.4

Release Notes

September 23, 2020

Contents

What's changed

Version	Change
September 23, 2020	Fourth maintenance release. See resolved issues. Hashes updated.
September 04, 2020	CSCvr13451 removed from Open Issues as it was resolved in 2.8.1.
June 25, 2020	Third maintenance release. See resolved issues. Hashes updated.
May 11, 2020	Open issues updated.
April 17, 2020	Minor corrections.
April 01, 2020	Second maintenance release. See resolved issues. Hashes updated.
February 20, 2020	First maintenance release. Default behavior for H.264 for Chromium browsers changed See resolved issues. Hashes updated.
December 03, 2019	OVA file hashes updated.
November 29, 2019	Added caution related to changing loadLimit value for Cisco Meeting Server 2000 in the section on Upgrading. Other minor edit.
November 13, 2019	New release of Cisco Meeting Server software.

1 Introduction

These release notes describe the new features, improvements and changes in release 2.8 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.

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.

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.

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.

1.2.3 Call capacities

Table 1 provides a comparison of the call capacities across the platforms hosting Cisco Meeting Server software version 2.8.

Table 1: Call capacities

Type of calls	Cisco Meeting Server 2000	Cisco Meeting Server 1000 M4	Cisco Meeting Server 1000 M5
Full HD calls (1080p30)	350	48	48
HD calls (720p30)	700	96	96
SD calls (448p30)	1000	192	192
Audio calls	3000	1700	2200

1 below compares the call capacities for a single or cluster of Meeting Servers compared to load balancing calls within a Call Bridge Group.

Cisco Meeting Server platform		Cisco Meeting Server 1000 M4	Cisco Meeting Server 1000 M5	Cisco Meeting Server 2000
Individual Meeting Servers or Meeting Servers in a cluster (notes 1,2 3 and 4)	1080p30 720p30 SD Audio calls	48 96 192 1700	48 96 192 2200	350 700 1000 3000
	HD participants per conference per server	96	96	450
	WebRTC connections per Web Bridge	100	100	100
Meeting Servers in a Call Bridge Group	Call type supported	Inbound SIP Outbound SIP Cisco Meeting App		
	1080p30 720p30 SD Audio calls Load limit	48 96 192 1700 96,000	48 96 192 2200 96,000	350 700 1000 3000 700,000
	Number of HD participants per conference per server	96	96	450
	WebRTC connections per Web Bridge	100	100	100

Note 1: Maximum of 24 Call Bridge nodes per cluster; cluster designs of 8 or more nodes need to be approved by Cisco, contact Cisco Support for more information.

Note 2: Clustered Cisco Meeting Server 2000's without Call Bridge Groups configured, support integer multiples of maximum calls, for example integer multiples of 700 HD calls.

Note 3: Up to 16,800 HD concurrent calls per cluster (24 nodes x 700 HD calls).

Note 4: A maximum of 2600 participants per conference per cluster depending on the Meeting Servers platforms within the cluster.

Note 5: 1 assumes call rates up to 2.5 Mbps-720p5 content for video calls and G.711 for audio calls. Other codecs and higher content resolution/framerate will reduce capacity. When meetings span multiple call bridges, distribution links are automatically created and also count against a server's call count and capacity. Load limit numbers are for H.264 only.

Note 6: VMware have made changes in their recent versions (6.0 update 3, 6.5 update 2 and 6.7) that has reduced the throughput of audio calls on Cisco Meeting Server version 2.8 and later (video capacity is unaffected).

1.3 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.

1.4 End of Software Maintenance

On release of Cisco Meeting Server software version 2.8, Cisco announces the time line for the end of software maintenance for the software in Table 2.

Table 2: 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 2.6.x	4 months after the first release of Cisco Meeting Server version 2.8.

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

2 New Features/Changes in version 2.8

Version 2.8 of the Meeting Server software, adds the following:

- Customizable layouts to allow Administrators more flexibility to create and apply custom layouts that suit their specific needs.
- Far end camera control (FECC) support to all SIP endpoints that support FECC, allowing administrators to remotely control the camera at the far end.
- Audio prompts for lock/unlock meeting status and how many participants are in the meeting.
- ability to enable Automatic Gain Control (AGC). This is a beta feature only in this release.
- ESXi support improvements on M4 and specs-based servers for ESXi 6.7 and ESXi6.5 Update 2 and later builds.
- ability to disable peer to peer ICE negotiation.
- an increase in the maximum size of packet capture to 1GB.

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.

2.1 New features introduced in version 2.8.1

In 2.8.1 the default behavior for H.264 for Chromium browsers is changed to allow 1080p main and content streams to be decoded using Chrome's software decoder, thereby improving the quality and user experience of the meeting.

2.2 Customizable Layouts

From version 2.8, Meeting Server introduces customizable layouts. This allows Administrators more flexibility to create and apply custom layouts that suit their specific needs. This feature can work on single and dual screen endpoints.

Note: Customizable layouts are not supported on triple screen endpoints.

Note: Customizable layouts is a licensed feature. You need to purchase the necessary license to use this feature – it's an option under A-CMS (Cisco Meeting Server subscriptions) and is a subscription that can be used alongside existing perpetual or subscription licenses.

We allow configuration of custom layouts with or without the license key, however without the key Meeting Server will behave as though no custom layout is configured.

Note: Customizable layouts do not apply to Cisco Meeting App or Microsoft clients joining a dual homed conference. Customizable layouts will apply if the Microsoft client joins Meeting Server directly.

Example layouts are available to demonstrate the capabilities of customizable layouts and how to create your own. For more information about example layouts and JSON text files, see Appendix A.

The following information applies to customizable layouts:

- Administrators can apply customizable layouts on a call leg profile basis.
- Customized layouts define what users see, for example, how many participants are displayed, where the participants are displayed, and how big each participant's pane is.
- Existing conference layout restrictions still apply, such as a maximum of 25 participants are displayed on a single endpoint; and a default of 4 remote video streams per remote Call Bridge in a clustered deployment (9 remote video streams across distribution links between clustered Call Bridges is still a preview feature).
- Existing icons / audio prompts will work with customizable layouts.

To support this new feature the following new API objects are introduced in version 2.8:

- **`/layoutTemplates`**
- **`/layoutTemplates/<layout template id>`**
- **`/layoutTemplates/<layout template id>/template`**

2.2.1 Licensing for using customizable layouts

A new API parameter **`customizations`** on **`/system/licensing`** is introduced in version 2.8 to support customizable layouts. The value is available upon issuing a GET command.

2.2.2 How to implement customizable layouts

1. Create your own customized layout template file (JSON text file) using a text editor – you can use a custom layout example supplied by Cisco here. (More information about JSON text file layouts can be found in Appendix A .)
2. Create and give a name to a layout template node with a string parameter **`name`** using the API:
    - POST to **`/layoutTemplates`**

3. Assign a JSON layout description to this new layout template node:
   - PUT to **/layoutTemplates/<layout template id>/template** with MIME type set to **application/json**
4. Apply a **layoutTemplate** to a callLegProfile and have that used for call legs to which this profile applies.
   - PUT to **/callLegProfiles/<call leg profile id>** or POST to **/callLegProfiles**

   The customized layout template takes the place of the automatic layout in the set of layouts available to the endpoint.

   For example, if you set **defaultLayout** to **automatic** in a **callLegProfile** that also configures a **layoutTemplate** GUID, all active call legs using that **callLegProfile** will switch to display the custom layout. ActiveControl endpoints can change to or from the customized layout by selecting or deselecting **automatic** as appropriate.

   Note: Set the layout to **automatic** to get the newly-uploaded custom layout to be used in a live conference.

2.2.3 API failure reasons

The new **layoutTemplates** API object can produce the following new API failure reasons:

- **layoutTemplateDoesNotExist** – if the layout template GUID is not recognized.
- **layoutTemplateDescriptionTooLong** – if the proposed layout template description is too long.

2.2.4 Setting / overriding a layout template on a call leg

Each call leg profile parameter can be overridden by specifying a value for the parameter directly on a call leg API object. The new parameter **layoutTemplate** is added to callLeg objects. This new parameter supports the following operations:

- POST to **/calls/<call id>/callLegs** or PUT to **/callLegs/<call leg id>**
- GET on **/callLegs/<call leg id>**

2.2.5 Overriding a layout template on a participant

So that API operations on a participant's call legs can be issued from a Call Bridge different to the one where the call legs are homed, the new parameter **layoutTemplate** is introduced on participant objects.

To allow overriding of the effective call leg profile settings in the participant's call legs:

- POST to **/calls/<call id>/participants**

Support for GET on the 'participants' API node is as follows:

- GET on **/participants/<participant id>** can give the response parameters **layoutTemplate** and **defaultLayout**. Both response parameters reflect the values from the effective call leg profile for both local and remote participants and are nested under **configuration** in the response entry.

2.2.6 Getting information for the layout template on an active call leg

You can retrieve information about an active call leg for local participants by using GET on **/callLegs/<call leg id>**. The response has nested subsections **configuration** and **status**, each of which contains the new parameter:

- **layoutTemplate [<layout template id> | ""]**

The value of **layoutTemplate** in the **configuration** subsection reflects the value in the resultant call leg profile, whereas the one in the **status** subsection specifies which template is actually used. For example, if there is no valid license, the value under **status** would be absent despite potentially being present under **configuration**.

2.2.7 Turning off a customized layout template

On the objects where **layoutTemplate** has a template ID set, change the setting to **""**. If the customized layout template is turned off, the layout will switch back to its default behavior.

2.3 Far end camera control

Cisco collaboration uses technology such as SpeakerTrack, PresenterTrack and best overview to intelligently and automatically frame the correct people in a meeting. Sometimes the endpoints in a meeting do not support this or manual control is required. From 2.8, Meeting Server implements far end camera control (FECC) for SIP endpoints that support FECC to solve these use cases.

When Meeting Server receives FECC, it forwards FECC commands to the participant in the "main pane", provided the participant sending FECC has permissions to control the far end camera and the far end supports FECC.

The "main pane" is a defined focused pane for each layout – usually the biggest pane. With pane placement or importance in use, this means that FECC is sent to the highest importance participant. You can use importance to determine who the FECC is sent to.

Note: Existing methods of selecting a layout or determining (for example, by importance) who is shown in the main pane can be used.

Note: Where there is a defined main pane, you can use FECC to control the far end camera of the system in that main pane. However, where a layout doesn't have such a main pane, such as a multi-pane allEqual layout, you can't use FECC.

When a participant chooses to control the far end camera of the main pane, if that main pane has "advertised" it supports FECC, a highlighted border displays around that main pane for the duration that the participant sends camera control commands to it using the controls available on their endpoint. The highlighted border only displays to the participant controlling the camera.

Note: If in a point-to-point meeting then each participant can potentially control each others camera.

FECC is enabled by default on Meeting Server, so should require no further configuration. To support FECC the following new API parameters are introduced in version 2.8:

`controlRemoteCameraAllowed` with possible values **`true`** and **`false`** is added to:

- GET and PUT **`/callLegs/<callLeg id>`** . Also POST for **`/callLegs`**
- GET and PUT **`/callLegProfiles/<call leg profile id>`**. Also POST on **`/callLegProfiles`**
- POST on **`calls/<call id>/participants`**

To view the **`controlRemoteCameraAllowed`** value for a participant:

- GET on **`/callLegs/<call leg id>`** or **`/callLegProfiles/<call leg profile id>`**.

`sipH224` with possible values **`true`** (default) and **`false`**. This parameter controls whether the use of H.224 is allowed within SIP calls (this protocol is used for FECC support). This parameter is added to:

- POST on **`/compatibilityProfiles`**
- PUT on **`/compatibilityProfiles/<compatibility profile id>`**
- GET on **`/compatibilityProfiles/<compatibility profile id>`**

If the compatibility profile for **`sipH224`** is not set then FECC will be sent by default.

Note: At the time of writing, whilst the touch panel for CE endpoints does support sending FECC commands in point-to-point modes it does not offer this interface when connected to a meeting on Meeting Server. However, FECC commands can be sent from the web interface for the endpoint.

2.4 Audio prompts (lock/unlock meeting and number of participants)

From 2.8, Meeting Server introduces new audio prompts for the following:

2.4.1 Lock / unlock status of the meeting

The audio prompt "this meeting is locked" plays to all participants who are actively participating in the meeting when it is locked.

When unlocking a meeting the audio prompt "this meeting is unlocked" plays to all participants who are actively participating in the meeting.

Note that the lock/unlock audio prompts only play on state change.

To use the new audio prompts, the following new files can be used / customized: "meeting_locked.wav" and "meeting_unlocked.wav".

For more information, see the Customization Guidelines.

2.4.2 Number of participants in the meeting

Previously, audio-only participants had no idea how many participants were in a conference. From 2.8, you can enter a DTMF command to find out how many participants are actively participating in a meeting. The command responds with a number up to 20: "There are n participants in the meeting"; and if more than 20, the response is "There are more than 20 participants in the meeting".

If someone leaves or joins after the DTMF command then participants can use the beep on join/leave feature to be notified that the attendance has changed and then press the DTMF command again.

The number of participants value is the total participants actively participating in the meeting including the participant that initiates the command. If a participant is locked in the lobby, they are not included in the participant count. The audio prompt is only played to the participant that initiates the command.

To implement this new feature the API DTMF profile method supports a new parameter: **`getTotalParticipantCount`**. This parameter allows a DTMF string to be configured in a DTMF profile and applied (for example, as a system profile) so that when the DTMF command is entered by any participant an audio prompt of the total number of participants in the meeting is heard.

To implement this audio prompt:

- POST to **`/dtmfProfiles`** and set the field **`getTotalParticipantCount`** to a DTMF sequence (e.g. **9#)

Note: The number of participants audio prompt will not work in forwarded calls, for example, SIP to SIP, Skype to SIP. The reason for this is that in any gateway call the DTMF is forwarded but not processed by the Meeting Server.

These new audio prompts are customizable via locally-hosted and remotely-hosted branding. They are also available in localized format together with the other supported Meeting Server audio prompts.

Note: These new audio prompts play to all meeting participants, including video participants. However, they do not play in an AVMCU meeting, or to Cisco Meeting App participants .

2.5 Ability to enable Automatic Gain Control (AGC) (beta feature)

Due to different audio levels being set by third party clients and the variation in audio levels from different headsets, conferences can often have participants that sound too loud or too quiet. Meeting Server uses Automatic Gain Control (AGC) to adjust audio level that it receives from individual participants in order to deliver as consistent an audio level across the conference as possible.

From 2.8, Meeting Server introduces Automatic Gain Control (AGC) on audio received by the Meeting Server. (It is not on audio transmitted by the Meeting Server.)

AGC will be applied to any endpoint (physical endpoints or soft clients) connected directly to the Meeting Server. It will not be applied to TIP calls or AVMCU (because this is a mixed audio stream).

Note:

- Skype participants connected to AVMCU will not be subject to any AGC as the AVMCU controls the audio.
- AGC is not applied to distribution links between Meeting Servers because this is a mixed audio stream.

Note: Although enabling AGC is marked as "beta", we are confident in the stability of this feature and would like to encourage you to deploy it in a production environment. Due to the nature of trying to recreate scenarios to test this feature thoroughly in a test environment, this feature has not had as much "real world testing" as we would like. Should you see any issues, please disable the feature and raise a TAC support case. It is intended that this feature will be turned on as default after it has had more testing in production environments. We welcome any feedback you may have on this feature.

AGC is disabled by default and can only be enabled via the new parameter **`audioGainMode`**, with possible options **`agc`** and **`disabled`**. This new parameter is supported on these APIs:

- GET and PUT operations on **`/callLegProfiles/<call leg profile id>`** and also POST on **`/callLegProfiles`**
- GET and PUT operations on **`/callLegs/<call leg id>`** and also POST on **`/callLegs`**
- GET and PUT operations on **`/calls/<call id>/callLegs`**

When AGC is enabled, the gain applied will be visible on the **Status > Calls** webadmin page. Also, there is a new API parameter **`gainApplied`** which is returned in response to a GET operation on **`/callLegs/<call leg id>`** under the **`rxAudio`** section.

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.

2.6 ESXi support

Version 2.8 adds support on M4 and specs-based servers for:

- ESXi6.7
- ESXi6.5 Update 2 and later builds.
- ESXi 6.0 Update 3

VMware have made changes in their recent versions (ESXi 6.0 update 3, 6.5 update 2 and 6.7) that have reduced the throughput of audio calls on Cisco Meeting Server in version 2.8 (video capacity is unaffected). This table shows the new 2.8 call capacity figures.

Note: The capacity figures assume the use of the default ESXi scheduler rather than either version of the SCA (Side Channel Aware) schedulers. (ESXi 6.7 adds a second version of the scheduler.)

Table 3: Call capacities

Type of calls	Cisco Meeting Server 1000 M4	Cisco Meeting Server 1000 M5
Full HD calls (1080p60)	24	24
Full HD calls (1080p30)	48	48
HD calls (720p30)	96	96
SD calls (448p30)	192	192
Audio calls	1700	2200

Note: Meeting Server 2000 and X series do not use VMware and so are unaffected and have no change in capacity.

2.7 Ability to disable peer-to-peer ICE negotiation

In certain network scenarios it is desirable to be able to disable peer-to-peer ICE negotiation. Version 2.8 introduces the new API parameter **`distributionLinkMediaTraversal`** to control whether media traversal (ICE / STUN) should be used for distribution links between clustered Meeting Servers.

This new API parameter is enabled by default but can be set to disabled if the media flow doesn't support ICE candidates and you want to ensure that media traversal should not be used for distribution links.

If this parameter is not set then the behavior will default to allow peer-to-peer ICE negotiation. If peer-to-peer ICE negotiation is enabled the behavior will be the same as in previous releases.

It can be set in **/compatibilityProfiles** and is set globally, i.e. for all Call Bridges in the cluster connected to the Database provided you create or modify a compatibilityProfile object and ensure that profile is set at the **/system/profiles** level.

This new API parameter, **distributionLinkMediaTraversal** with possible values **enabled** (default) and **disabled**, is added to:

- POST on **/compatibilityProfiles**
- PUT on **/compatibilityProfiles/<compatibility profile id>**
- GET on **/compatibilityProfiles/<compatibility profile id>**

2.8 Serviceability improvement

Version 2.8 introduces an increase in the maximum size of packet capture obtainable to 1GB from the previous maximum of 100MB.

2.9 Summary of API Additions and Changes

New API functionality for the Meeting Server 2.8 includes:

- new API object and parameters to customize layouts on the Meeting Server.
- new API DTMF profile method to implement the new audio prompt for the number of participants in the meeting.
- new API parameter **controlRemoteCameraAllowed** and **sipH224** to support Far End Camera Control (FECC).
- new API parameter **distributionLinkMediaTraversal** to provide ability to disable peer-to-peer ICE negotiation
- new API parameters **audioGainMode** to enable Automatic Gain Control (beta feature) and **gainapplied** to view status on callLegs.

2.9.1 Using customized layout templates

This is a brief summary of the new API functionality introduced in 2.8 to support customized layouts.

- New API objects are introduced:
  - **/layoutTemplates**
  - **/layoutTemplates/<layout template id>**
  - **/layoutTemplates/<layout template id>/template**
- support for the new API object **layoutTemplates** and string parameter **name** as follows:
  - POST to **/layoutTemplates** or PUT to **layoutTemplates/<layout template id>**
  - Enumerate: GET on **/layoutTemplates** supporting the standard URI parameters **limit**, **offset** and **filter**
  - Retrieve: GET on **/layoutTemplates/<layout template id>**
  - DELETE on **/layoutTemplates/<layout template id>** (note, DELETE is not on **/layoutTemplates/<layout template id>/template**)
- new response parameter **templateSize** is available on the Enumerate and Retrieve operations to indicate the size in bytes of the layout template description.
- support for the new API node **/layoutTemplates/<layout template id>/template** as follows:
  - PUT to **/layoutTemplates/<layout template id>/template** with MIME type set to **application/json** to assign a JSON layout description to this new layout template node.
  - GET on **/layoutTemplates/<layout template id>/template** to retrieve the layout template description associated with a layout template. An optional URI parameter **source** can be specified on the GET operation. If it's not provided, the GET operation returns the original JSON description as given on the PUT on **/layoutTemplates/<layout template id>/template**.
- new parameter added to callLegProfile objects: **layoutTemplate [<layout template id> | ""]**
- new parameter added to callLeg object: **layoutTemplate [<layout template id> | ""]**. This new parameter supports the following operations:
  - POST to **/calls/<call id>/callLegs**
  - PUT to **/callLegs/<call leg id>**
  - GET on **/callLegs/<call leg id>**
- new parameter added to callLegProfiles object: **layoutTemplate [<layout template id> | ""]**. This new parameter supports the following operations:
  - POST to **/callLegProfiles**
  - PUT to **/callLegProfiles/<call leg profile id>**

  - GET on **/callLegProfiles/<call leg profile id>**
- new parameter added to participants object: **layoutTemplate [<layout template id> | ""]**. This new parameter supports the following operation:
  - POST to **/calls/<call id>/participants**
- new API failure reasons added:
  - **layoutTemplateDoesNotExist**
  - **layoutTemplateDescriptionTooLong**
- new parameter is added to the response for information about an active call leg using GET on **/callLegs/<call leg id>**. The nested subsections **configuration** and **status** contain the new parameter:
  - **layoutTemplate [<layout template id> | ""]**
- new response parameters **layoutTemplate** and **defaultLayout** available using GET on **/participants/<participant id>**
- new response parameter **customizations** available using GET on **/system/licensing**

2.9.2 Creating a layout template node with **layoutTemplates**

To create a layout template node:

- POST to **/layoutTemplates** supplying a name for the layout template with a string parameter **name**

To assign a JSON file layout description to the new node,

- PUT on **/layoutTemplates/<layout template id>/template** with MIME type set to **application/json**

2.9.3 Associating a custom layout template with a call leg profile

To apply a **layoutTemplate** to a callLegProfile so that it is used for call legs to which that profile applies:

- PUT to **/callLegProfiles/<call leg profile id>** or POST to **/callLegProfiles**.

The customized layout template takes the place of the automatic layout in the set of layouts available to the endpoint.

For example, if you set **defaultLayout** to **automatic** in a **callLegProfile** that also configures a **layoutTemplate** GUID, all active call legs using that **callLegProfile** will switch to display the custom layout. ActiveControl endpoints can change to or from the customized layout by selecting or deselecting **automatic** as appropriate.

Note: Set the layout to "automatic" to get the newly-uploaded custom layout to be used in a live conference.

For a call leg, if **defaultLayout** is set to **automatic**, **layoutTemplate** contains an ID of a valid layout template, and the Call Bridge has a valid license for using custom layouts, then the custom layout is enforced to the call leg. If the layout template is unset or deleted while in force, **automatic** switches to its default behavior.

The parameter supports the following operations:

- POST to **/callLegProfiles**
- PUT to **/callLegProfiles/<call leg profile id>**

To retrieve the **layoutTemplate** value on a callLegProfile object, use GET on **/callLegProfiles/<call leg profile id>**

2.9.4 Setting / overriding a layout template on a call leg

To set or override a customizable layout template on a call leg:

- POST to **/calls/<call id>/callLegs** the request parameter **layoutTemplate**
- PUT to **/callLegs/<call leg id>** the request parameter **layoutTemplate**

To retrieve the **layoutTemplate** value on a callLeg object, use GET on **/callLegs/<call leg id>**

2.9.5 Retrieving information for the custom layout template on an active call leg

You can retrieve information about an active call leg by using GET on **/callLegs/<call leg id>**. The response structure includes the nested subsections **configuration** and **status** which contain the new parameter **layoutTemplate [<layout template id> | ""]**

This parameter will be present in **status** if a custom layout template is currently being used to generate the layout for the call leg, and if so, it identifies which layout template is being used.

The value of **layoutTemplate** in the **configuration** subsection reflects the value in the resultant call leg profile, whereas the one in the **status** subsection specifies which template is actually used. For example, if there is no valid license, the value under **status** would be absent despite potentially being present under **configuration**.

2.9.6 Overriding a layout template on a participant

So that API operations on a participant's call legs can be issued from a Call Bridge different to the one where the call legs are homed, the new parameter **layoutTemplate** is introduced on participant objects.

To allow overriding of the effective call leg profile settings in the participant's call legs:

- POST to **/calls/<call id>/participants**

2.9.7 Retrieving information for the custom layout template for participants

You can retrieve information about a participant as follows:

- GET on **/participants/<participant id>** can give the response parameters **layoutTemplate** and **defaultLayout**. Both response parameters reflect the values from the effective call leg profile for both local and remote participants and are nested under **configuration** in the response entry.
  - **layoutTemplate [<layout template id>]**
  - **defaultLayout**: one of:
    - allEqual
    - speakerOnly
    - telepresence
    - stacked
    - allEqualQuarters
    - allEqualNinths
    - allEqualSixteenths
    - allEqualTwentyFifths
    - onePlusFive
    - onePlusSeven
    - onePlusNine
    - automatic
    - onePlusN

2.9.8 Licensing for using custom layouts

To retrieve the licensing information for using custom layouts, use GET on **/system/licensing**, the response **features** includes the new response parameter **customizations**.

2.9.9 Implementing the audio prompt for total number of participants in a meeting

The API DTMF profile method supports a new parameter: **getTotalParticipantCount**. This parameter allows a DTMF string to be configured in a DTMF profile and applied (for example, as a system profile) so that when the DTMF command is entered by any participant an audio prompt of the total number of participants in the meeting is heard:

To implement the audio prompt:

- POST to **dtmfProfiles** and set the field **getTotalParticipantCount** to a DTMF sequence (e.g. **9#),
- PUT to **/dtmfProfiles/<dtmf profile id>**

2.9.10 Using Far End Camera Control

FECC is enabled by default from 2.8 on Cisco Meeting Server. However, the following API additions and changes are introduced, if required:

The **controlRemoteCameraAllowed** parameter with possible values **true** and **false** is added to:

- GET and PUT **/callLegs/<call leg id>** . Also POST for **/callLegs**
- GET and PUT **/callLegProfiles/<call leg profile id>**. Also POST on **/callLegProfiles**
- POST on **calls/<call id>/participants**

To view the **controlRemoteCameraAllowed** value for a participant use GET on **/callLegs/<call leg id>** or **/callLegProfiles/<call leg profile id>**.

sipH224 has possible values **true** (default) and **false**. This parameter controls whether the use of H.224 is allowed within SIP calls (this protocol is used for FECC support). This parameter is added to:

- POST on **/compatibilityProfiles** the request parameter **sipH224** set to the chosen value of **true** or **false**.
- PUT on **/compatibilityProfiles/<compatibility profile id>** the request parameter **sipH224** set to the chosen value of **true** or **false**.

To retrieve the **sipH224** value on a compatibility profile, use GET on **/compatibilityProfiles/<compatibility profile id>**

2.9.11 Retrieving information on whether camera control is available on an active call leg

You can retrieve information about an active call leg by using GET on **/callLegs/<call leg id>**. The response structure includes the nested subsection **status** which contains the new parameter:

- **cameraControlAvailable** [**true** | **false**]

This indicates whether this call leg has advertised the ability for its camera to be controlled remotely:

- **true** – camera control for this call leg is possible
- **false** – camera control for this call leg is not possible

2.9.12 Retrieving information on whether camera control is available for a participant

You can retrieve information about an active call leg by using GET on **/participants/<participant id>**. The response structure includes the nested subsection **status** which contains the new parameter:

- **cameraControlAvailable** [**true** | **false**]

This indicates whether this participant has advertised the ability for its camera to be controlled remotely:

- **true** – camera control for this participant is possible
- **false** – camera control for this participant is not possible

2.9.13 Disabling peer-to-peer ICE Negotiation

To disable peer-to-peer ICE negotiation:

- POST to **/compatibilityProfiles** the request parameter **distributionLinkMediaTraversal** set to **disabled**
- PUT to **/compatibilityProfiles/<compatibility profile id>** the request parameter **distributionLinkMediaTraversal** set to **disabled**

To retrieve the **distributionLinkMediaTraversal** value on a compatibility profile, use GET on **/compatibilityProfiles/<compatibility profile id>**

2.9.14 Enabling Automatic Gain Control (AGC)

To enable AGC:

- PUT to **/callLegProfiles/<call leg profile id>** the parameter **audioGainMode** set to **agc**
- POST on **/callLegProfiles** the parameter **audioGainMode** set to **agc**

To retrieve the **audioGainMode** value on callLegProfiles, use GET on **/callLegProfiles/<call leg profile id>**

- PUT to **/callLegs/<call leg id>** the parameter **audioGainMode** set to **agc**
- POST on **/callLegs** the parameter **audioGainMode** set to **agc**

To retrieve the **audioGainMode** value on callLegs, use GET on **/callLegs/<call leg id>**, the parameter **gainApplied** is returned in the response under the **rxAudio** section.

- PUT operations to **/calls/<call id>/callLegs** the parameter **audioGainMode** set to **agc**

To retrieve the **audioGainMode** value on calls, use GET on **/calls/<call id>/callLegs**

To retrieve the **audioGainMode** value on a call leg profile use GET on **/callLegs/<call leg id>/callLegProfileTrace>**. The parameter **audioGainMode** is returned in the response structure under **callLegProfile** in the nested subsection **profile**.

2.10 Summary of MMP changes

There are no new additions or changes to the MMP commands for version 2.8.

2.11 Summary of CDR Changes

There are no new CDR records or parameters for version 2.8.

2.12 Summary of Event Changes

There are no new Events for version 2.8.

3 Upgrading, downgrading and deploying Cisco Meeting Server software version 2.8

This section assumes that you are upgrading from Cisco Meeting Server software version 2.7. If you are upgrading from an earlier version, then Cisco recommends that you upgrade to 2.7 first following the instructions in the 2.7.x release notes, before following any instructions in these Cisco Meeting Server 2.8 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 2.7.

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 2.8

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. If you have already increased the loadLimit value when you installed version 2.6, then no further increase is required.

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 the 2.6 release notes. 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_8_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:
   d1fc5de02d1faa53843e579d74ebc0b43a39e77207d785c4c80ee35f27eb1b55

   `Cisco_Meeting_Server_2_8_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:
   d191453d7608cc551ec80d6706a137db12cb6b01705e1deac19fece40005f889

   `Cisco_Meeting_Server_2_8_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:
   d7e9cebf7bc003e384779c44322f0667c459b2a5e7871896c0a48cdcf83aa8b5

   `Cisco_Meeting_Server_2_8_4.ova`

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

   For vSphere6, hash (SHA-512) for Cisco_Meeting_Server_2_8_4_vSphere-6_0.ova file:
   8e0b5606a078e57fd69dbd5fba4c2f3aeae07f707b4b02d8c47ad6b755a30bc63f4f58285434b0450fcdad95c4be342b7234af23a210d0a8458586be077c1df2

   For vSphere6.5 and higher, hash (SHA-512) for Cisco_Meeting_Server_2_8_4_vSphere-6_5.ova file:
   a4cee2b469a3e6fdec284a646263b81ee99799ef76c22969a07ee02c0789dbdeb6c9a133d1e94749ee91ef237590cf4c4aaceb98bc0e612e5688f2bb75ee7ffd

2. To validate the OVA file, the checksum for the 2.8.4 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 and 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 and 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 2.8 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 `2.8`.
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

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 2.8.4

Cisco identifier	Summary
CSCvv01243	TURN chooser behavior is restored following the fix for the Expressway issue CSCvu85005.
CSCvu70860	Meeting Server may experience an unexpected restart if ICE and Multistream are used together in a call.
CSCvu42590	When a Cisco Meeting App (desktop, iOS and WebRTC) user joins a meeting with lock/unlock permissions, if they lock the meeting and sign out, and then rejoin the same meeting and try to unlock, the meeting remains locked.

Issues seen in previous versions that are fixed in 2.8.3

Cisco identifier	Summary
CSCvu59965	If there are two outbound rules for for the same proxy but targeted for SIP and Lync respectively, depending on the priority of the rules, Meeting Server may not add essential information in the outgoing SIP INVITE (Ms-Conversation-ID) for the Lync call. This results in the outbound Lync call to fail.
CSCvu47594	When Meeting Server is under load an unexpected restart can occur when a participant (Participant X) uses XCCP (Active control) to disconnect another person (Participant Y), and shortly after they (Participant X) leave the call.
CSCvu67565	In rare circumstances, sharing presentation from Lync or Skype-for-Business client to Meeting Server can result in the Meeting Server encountering an unexpected restart.
CSCvu29634	Joining meetings intermittently fails when Meeting Server is sent a Re-INVITE from Cisco Unified Communications Manager.
CSCvu14250	Distortion and video corruption can be seen on SIP calls where just the branding background image is displayed and that image has not been subsampled at 4:2:0 or 4:2:2 format.
CSCvu03895	On rare occasions when H.224 traffic is being sent and received whilst the H.224 call is being destroyed a Mutex lockup and an unexpected restart occurs.
CSCvt99690	Multiple Call Bridges can overload a recorder and exceed its recording capacity. When this happens, the recorder runs out of memory and an unexpected restart occurs.
CSCvt92941	During a pairing operation between an endpoint and Webclient, an invalid token in a SIP URI causes a parsing error, which in turn causes all XMPP/WebRTC calls to drop across the Meeting Server.
CSCvu23273	A mutex long lock results in circumstances that can cause the Meeting Server to experience unexpected restarts.
CSCvt91847	In rare circumstances, all participants can unexpectedly drop from a Meeting Server due to inconsistent lock status between local and remote Call Bridges in a distributed conference.
CSCvt62395	The participant count on WebRTC page might count incorrectly for new comers after the total number of WebRTC participants exceeded 100.
CSCvt91472	In rare circumstances, the Meeting Server can unexpectedly restart when XMPP issues are occurring on the server.
CSCvu36836	When a Skype client is presenting in a dual-homed call, the receiving SIP endpoint can sometimes see incorrect username for the Skype presenter on the endpoint's touch panel display or participant drop-down list. This only affects Active-Control enabled SIP endpoints.
CSCvt86179	In rare circumstances, a very busy Meeting Server can unexpectedly restart when performing a variety of call control and sync operations.

Cisco identifier	Summary
CSCvt76282	On rare occasions, Meeting Server may unexpectedly restart when de-instantiating a Cisco Meeting App user (WebRTC user included).
CSCvt59193	In rare circumstances, a race condition can occur during XMPP message processing, resulting in the Meeting Server unexpectedly restarting .

Issues seen in previous versions that are fixed in 2.8.2

Cisco identifier	Summary
CSCvt60966	Cisco Meeting Server 2000 media blade experiences MCE events which can cause a CMCI (Corrected Machine Check Interrupt) storm.
CSCvt38067	In rare circumstances an unexpected restart may occur causing active calls to drop.

Issues seen in previous versions that are fixed in 2.8.1

Cisco identifier	Summary
CSCvs48726	After upgrading to Meeting Server version 2.8, calls are disconnected by VCS which gives the error message"Invalid syntax while parsing Session Description Protocol, expected".
CSCvs74975	An unexpected restart can occur when the user logs in to Meeting App and joins a conference using a SIP device (rather than on the client itself).
CSCvs09008	Meeting Server may suddenly restart when receiving content from a Microsoft Skype for Business user in a dual home call.
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.
CSCvs42333	Meeting Server may suddenly restart when sharing content with a Microsoft Skype for Business meeting.
CSCvs12175	Calls to Skype For Business may fail when the FQDN for a specific Meeting ServerCall Bridge is not specified in contact header when answering INVITE for invitation to AVMCU meeting.
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.
CSCvs08721	Skype participants video is not seen on SIP side of call when speaking.
CSCvr58520	Dual home calls and presentation calls may fail when Call Bridge answers the call sending the incorrect contact header in "200 Ok" response to Skype/Lync environment.
CSCvr13451	The Streamer disconnects and reconnects under packet loss conditions.
CSCvq81546	Significant packet loss and jitter reported by multiple endpoints on Meeting Server 2000.
CSCvs39544	Web Bridge fails to trust XMPP certificate which results in WebRTC call failure.
CSCvs96594	Call Bridge may unexpectedly restart when receiving content from Microsoft Skype for Business
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.

Issues seen in previous versions that are fixed in 2.8

Cisco identifier	Summary
CSCvq64378	On Cisco Meeting Server the Call Bridge up time is being reset silently. This doesn't affect normal operations.

Cisco identifier	Summary
CSCvr57767	The webadmin /log.html and /log.xml request does not always return the full xml text so the XML parsing fails.
CSCvo80460	Occasionally a SIP call is dropped by the far end due to an INVITE timeout.
CSCvs03934	Meeting Server running version 2.7 or below may unexpectedly restart when an unexpected Microsoft RDP sharing capability is received.
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.
CSCvr87685	Under certain circumstances you can't tell if a participant is locked in the lobby or not.

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
CSCvs04754	If a 3-screen TIP endpoint is dialed into a conference with a callLegProfile assigned to use a Layout Template and defaultLayout is set to auto, then the TIP endpoint will see the custom layout.
CSCvs04761	If the first participant to join the call is an activator then they will hear the message "This meeting is unlocked" (this happens with or without a pin).
CSCvs04746	Pane grouping issues with custom layouts. In custom layouts that have different sized panes, the Meeting Server tries to automatically assign the first big pane to "group 0" and the small panes to "group 1" for the purposes of placing active speakers in the view. However, where there are multiple big panes, this process can fail and lead to all panes being placed into a single group. Active speakers or participants marked as important can erroneously end up in small panes and not be correctly promoted to the layout's more prominent panes. As a work around, set the first small pane to be included in group 1 (with the JSON value "group": 1).
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.

Cisco identifier	Summary
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.
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.
CSCvh22816	Logging in using the WebRTC app may fail even when correct credentials are supplied. This occurs when a particular cookie string is supplied by the web browser to the Web Bridge. To avoid this happening either open an incognito tab to use the WebRTC app or clear all cookies for the domain used by the Web Bridge, for example for the WebRTC app at https://join.example.com, clear all example.com cookies.
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.

Appendix A JSON text file customizable layout example

From 2.8, the Meeting Server introduces customizable layouts. The definition for a customizable layout is contained within a JSON text file – the JSON file is uploaded and applied to a call leg profile as described in Section 2.2.

The JSON text file can contain customized layout definitions that describe anything from a single layout to an entire portfolio of multiple layouts.

Each individual customized layout in the portfolio is associated with a set of conditions that trigger the template to display. The set of conditions covers the number of video streams to show in the meeting, and the number of screens that the viewing endpoint is using. Every time one of these changes, for example, a participant joins or leaves the call or the number of screens changes, the portfolio gets re-evaluated and the (first) layout that satisfies all conditions will display. However, if no match is found then the layout reverts to the default "automatic" layout behavior.

Each layout definition within the JSON file has an array called "templates"; which in turn contains an array of objects. Each object represents a layout and the layout object contains two further objects:

- "conditions" section – defines the circumstances in which a layout will display.
  - "numScreens" – defines the number of screens across which the customized layout will display.
  - "minParticipants" and "maxParticipants" (optional) – determines when the layout applies, i.e. the range between "minParticipants" and "maxParticipants" is how many participants to show using this layout template.

    Note: "minParticipants" refers to the number of participant video streams that can be shown in your view (not the number of participants in the conference). The number discounts anyone not visible (e.g. audio only) and will only include yourself if you're using pane placement with self-view mode.

- "panes" array – contains the description for the position of every pane in the layout. The order the panes appear in the JSON text file corresponds to the sequence the panes will display in the layout. If there are fewer participant video streams than there are panes, then the first panes are used.

  The units are 0...1 where 1 is the full width or height of one screen. The code example below shows the positioning of the centered large pane where the mandatory values "left", "right", "upper", "lower" describes the position of the pane edges:

```
        "panes": [
    {
      "left": 0.20,
      "right": 0.80,
      "upper": 0.25,
      "lower": 0.75
    }
  ]
```

The "panes" array can also contain optional values per-pane for:

- "group" – supports 2 groups, 0 and 1. The group value determines the prominence of that particular pane – **`"group": 0`** panes should be first. You then need to determine where you wish to place the first **`"group": 1`** pane.
- "layer" – **`"layer": 0`** places the pane as the bottom layer (can be considered as a "z" coordinate). Values of 1 or above place the pane "on top". (0 is assumed the default if you don't specify a value.)

Figure 1 example template has up to 14 smaller panes surrounding one large centered pane for a single screen, and Figure 2 up to 20 smaller panes surrounding two large panes for a two screen system (active speaker will display in the large panes).

Figure 1: Single screen example custom layout

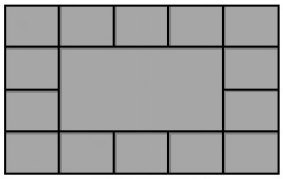
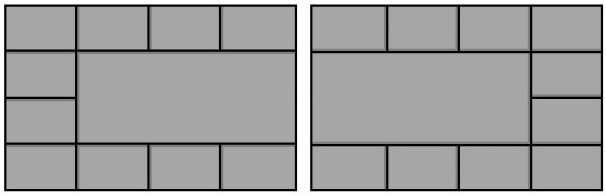


Figure 2: Dual screen example custom layout



Using these examples, the sequence that the panes are displayed as participants join the meeting is shown in the figures below:

Figure 3: Single screen example custom layout pane numbering sequence

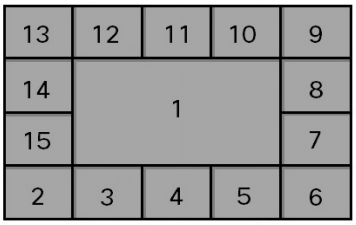
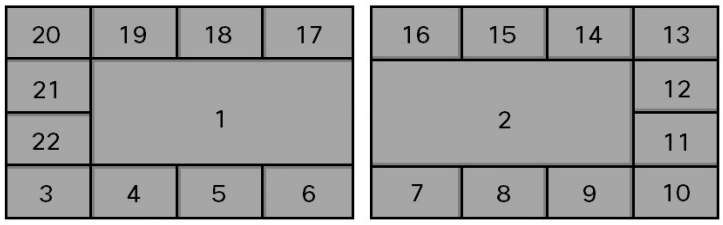


Figure 4: Dual screen example custom layout pane numbering sequence



An example JSON text file is attached to this PDF release note – locate and select the paperclip icon in Adobe Reader to view/edit. You can use this JSON text file to implement a customizable layout template to use "as is", or edit to customize further.

You can create your own layout, or use Cisco-supplied JSON template files to customize further to meet your needs. Example JSON template files can be found at https://github.com/ciscocms/layout-templates

Cisco Legal Information

Cisco Trademark