Cisco Meeting Server

Cisco Meeting Server Release 2.2.2

Release Notes

June 06, 2017

Contents

What's changed

Version	Change
2.2.2	Added section “Resolved in 2.2.2”.
2.2.1, June 2nd	Added support for Cisco Meeting Server 2000
2.2.1	Added section “Resolved in 2.2.1”.
2.2.0	New release.

1 Introduction

This release note describes the new features, improvements and changes in release 2.2.2 of the Cisco Meeting Server software for: specified servers based on Cisco UCS technology, Acano X-Series Servers, and virtualized deployments.

The Cisco Meeting Server was formerly called the Acano Server. The Cisco Meeting Server can be hosted on:

- the Cisco Meeting Server 2000, based on Cisco UCS technology running Cisco Meeting Server software as a physical deployment.
- 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.

The Cisco Meeting Server software is referred to as the Meeting Server throughout the remainder of this guide.

If you are upgrading from 2.1.x, 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 SIP edge: The Cisco Expressway X8.9 supports traversal of SIP traffic at the edge of the network, to and from the Cisco Meeting Server. You are encouraged to use the Cisco Expressway between remote Lync deployments and the Meeting Server, see the Cisco Expressway with Cisco Meeting Server and Microsoft Federation deployment guide.

The SIP and Lync Call Traversal feature first introduced in Acano Server release 1.8, is still a beta feature in Cisco Meeting Server 2.2, it is not intended for a production environment. This SIP edge feature will be withdrawn in version 2.3 of the Cisco Meeting Server software.

Cisco does not guarantee that a beta 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 about a single Edge solution for Cisco collaboration products: 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 Cisco Meeting Server H.323 Gateway component in six months' time, after which there will be no further development or feature releases related to the H.323 Gateway. Customers are encouraged to start evaluation of the more mature H.323 Gateway component in the Cisco Expressway, and plan their migration over.
The H.323 Gateway component will be removed from the Cisco Meeting Server software in a future release.

Note about rebranding the background image to the login page for the WebRTC app: From Meeting Server 2.1.2 the Meeting Server no longer supports the redesigned Web Bridge 2.0. Instead it supports Web Bridge 1.9 which does support rebranding the background image for the login page to the WebRTC app.

Note about message board chat: For existing deployments that use message board chat, chat will remain enabled when you upgrade to 2.2. 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.

2 New Features/Changes in 2.2

Release 2.2 of the software Meeting Server comprises:

- support for the Cisco Meeting Server 2000
- the capability to determine whether to display security icons on endpoints
- support for Office 365 dual homed experience with OBTP scheduling
- load balancing for outbound calls to SIP endpoints
- support for setting the maximum quality levels for main video and content
- improved DTMF comma handling
- layout and screen changes to improve user experience
- more control over UDP signaling for SIP
- diagnostic tools to help Cisco Support troubleshoot issues
- additional API objects and parameters to support these new features
- additional CDR support for new features.

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

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

2.1 Cisco Meeting Server 2000

The Cisco Meeting Server 2000 is a high performance, scalable platform for voice, video and web content, which integrates with a wide variety of third-party products from Microsoft, Avaya and other vendors. With the Cisco Meeting Server 2000, people connect regardless of location, device, or technology.

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. This gives better performance and utilizes the high performance capabilities of the UCS platform; a single Cisco Meeting Server 2000 supports up to 500 720p HD calls.

The Cisco Meeting Server 2000 is a core network device designed to handle a large number of calls. To support this capability only the Call Bridge, Web Bridge and XMPP server components are available for configuration. The Cisco Meeting Server 2000 is not suitable as an Edge server in a split Meeting Server deployment, because the TURN server and Load Balancer edge components are not available. Deployments that need firewall traversal support for external

Cisco Meeting App clients must deploy the TURN server and Load Balancer components on a separate Cisco Meeting Server 1000 or specification-based VM server.

In addition, the Recorder and Streamer components are not available on the Cisco Meeting Server 2000, as they are more suited to the lower capacity Cisco Meeting Server 1000 and specification-based VM servers.

The Cisco Meeting Server 2000 can be deployed as a single server on the internal network, as the core server in a single split server deployment, or one of multiple core nodes of a scalable deployment. It can be part of a deployment that includes Cisco Meeting Server 1000s, Acano X-series servers and specification-based VM servers, providing they are all running the same software version. The functionality, and user experience for participants, is identical across all platforms running the same software version.

For information on installing the Cisco Meeting Server 2000, see the Cisco Meeting Server 2000 Installation Guide. The Cisco Meeting Server 2000 is shipped with Cisco UCS Manager version 3.1(2f), and a version of Cisco Meeting Server software pre-installed. For information on upgrading UCS Manager to the latest version see this link and the Download software page. For information on upgrading Cisco Meeting Server software refer to Section 3.1. Note that the software for the Cisco Meeting Server 2000 is in a different upgrade file to VM deployments or the Acano X-series server.

2.2 Displaying security icons on endpoints

Some endpoints have the capability to render secure and unsecure padlocks to indicate whether the connection with the Meeting Server is secure. Prior to version 2.2, the Meeting Server also rendered an icon in the conference video to show whether the conference as a whole was secure. This could result in a user seeing two padlock icons, a closed one rendered by the endpoint and an open one rendered by the Meeting Server.

From version 2.2, the Meeting Server determines whether a connecting endpoint has the capability to render a security padlock representing the security status of the conference as a whole. If the endpoint does have the capability, then the Meeting Server will not send the icon to the endpoint. This ensures that the user will only ever see one padlock icon, and the endpoint controls whether a secure or unsecure icon is displayed. If the endpoint does not have the capability, then the Meeting Server will continue to send the appropriate padlock icon to the endpoint.

2.3 Office 365 Dual Homed Experience with OBTP Scheduling

Note: This feature requires the Call Bridge to connect to the public internet in order to contact Office 365. You need to open TCP port 443 on your firewall for outgoing traffic.

Version 2.2 supports “Office 365 Dual Homed Experience with OBTP (One Button To Push) Scheduling” allowing participants to join Office 365 meetings using Cisco endpoints that support OBTP. The feature requires version 2.2 on the Meeting Server combined with Cisco TMS 15.5, and Cisco TMS XE 5.5.

To set up this method of joining Office 365 meetings, configure the Meeting Server with an incoming dial plan rule with request parameter **`resolveToLyncSimpleJoin`** set to “true”. This tells the Meeting Server how to resolve the Lync Simple Meet URL sent in the Office 365 invite. To have the ability to call participants as well as meetings, use an existing outbound dial plan rule to route the outbound calls, or create a new outbound dial plan rule.

Note: If using Office 365, only invited OBTP-enabled endpoints or Skype for Business clients with Office 365 can join the Lync meeting; Cisco endpoints cannot join the meeting manually, via the Meeting Server IVR. This is a key difference to an on-premise Lync deployment,which allows any Cisco endpoint to join manually via the Meeting Server IVR.

2.3.1 Joining the meeting

The host schedules a meeting using Microsoft Outlook with Skype for Business plugin, and adds participants and conference rooms (including OBTP-enabled endpoints) and a location to meet in.

To join the meeting, participants using a OBTP-enabled endpoint simply push the OBTP button on the endpoint or touchscreen. Skype for Business clients click a link to join the meeting as normal.

2.3.2 In-conference experience

“Office 365 Dual Homed Experience with OBTP Scheduling” provides the “dual homed experience” with 2-way audio, video and content sharing. Office 365 clients have the familiar in-conference experience determined by the Lync AVMCU, and participants using OBTP-enabled endpoints have a video conferencing experience determined by the Meeting Server. All see the combined participants lists.

Note: Controls on clients do not work conference wide, and can give rise to some strange behavior. For example, if a Skype for Business client mutes an endpoint connected to the Meeting Server then the endpoint will mute, but no notification is sent to the endpoint to say it has been muted; the endpoint cannot unmute itself. If a Skype for Business client mutes all endpoints connected to the Meeting Server and then unmutes them, all the endpoints will remain muted.

Note: ActiveControl functionality such as muting and dropping participants only affect participants on the local Call Bridge and not on the Lync AVMCU.

2.4 Load balancing outbound SIP calls

From version 2.2, Call Bridge Groups supports the load balancing of outbound SIP calls, in addition to inbound SIP calls which was introduced in version 2.1.

To use this feature, do the following:

- enable load balancing of outbound SIP calls from spaces,
- set up outbound dial plan rules for load balancing outbound SIP calls.

Once load balancing is enabled, outbound SIP calls follow the logic:

- Find the highest priority outbound dial plan rule that matches the domain,
  - if this applies to a local Call Bridge, then balance the call within the local Call Bridge Group.
  - if this only applies to remote Call Bridges, then load balance the call within the Call Bridge Group to which the Call Bridge is a member.

However, you may prefer to supply the Call Bridge Group or a specific Call Bridge for the outbound SIP calls. In this situation, use the API object **`/calls/<call id>/participants`**, see below.

For more information on load balancing SIP calls across Call Bridge Groups, see the white paper: Load Balancing Calls Across Cisco Meeting Servers.

Note: Load balancing of calls from/to Lync clients, or Cisco Meeting Apps, is not currently supported by Call Bridge Groups.

2.4.1 How to enable load balancing of outbound SIP calls

To configure the Call Bridges in a specific Call Bridge Group to attempt to load balance outgoing SIP calls from spaces, perform a PUT on the API object **`/callBridgeGroups/<call bridge group id>`** with the **`loadBalanceOutgoingCalls`** parameter set to true. Use POST if setting up a new Call Bridge Group.

For load balancing of outbound calls, each Call Bridge in the group must have the same dial plan rules.

2.4.2 How to set up an outbound dial plan rule for load balancing outbound SIP calls

This can be achieved in 3 ways:

1. Setting the **`scope`** parameter to **`global`** in all of the outbound dial plan rules. This ensures that all Call Bridges are able to use all of the outbound dial plan rules to reach a matching domain.
2. Creating identical outbound dial plan rules for each Call Bridge in the Call Bridge Group. Set the **`scope`** parameter set to **`callBridge`**. Use the **`callBridge`** parameter to set the **`ID`** of the Call Bridge.
3. Creating outbound dial plan rules for the specific Call Bridge Group. Set the **`scope`** parameter to **`callBridgeGroup`**, and set the **`callBridgeGroup`** parameter to the **`ID`** of the Call Bridge Group.

Before using load balancing of outbound calls, review the existing dial plan rules for each Call Bridge in the Call Bridge group. If the scope of existing rules needs to be altered, perform a PUT on the API object **`/outboundDialPlanRules/<outbound dial plan rule id>`** supplying the scope request parameter as defined above. Use POST on the API object **`/outboundDialPlanRules`** if setting up a new outbound dial plan rule.

2.4.3 How to supply the Call Bridge Group or specific Call Bridge to use for outbound SIP calls to participants

To make a call from a specific Call Bridge Group, perform a POST on the API object **`/calls/<call id>/participants`** with the parameter **`callBridgeGroup`** and the **`ID`** of the Call Bridge group to use.

To make a call from a specific Call Bridge, perform a POST on the API object **`/calls/<call id>/participants`** with the parameter **`callBridge`** and the **`ID`** of the Call Bridge to use.

2.4.4 Handling load balancing of active empty conferences

The load balancing algorithm preferentially places new calls onto a Call Bridge where the conference is already active. An empty conference can be started on a Call Bridge by performing a POST on the API object **`/calls`**. By default these empty conferences are treated as active. This means that the first call to the empty conference is preferentially load balanced to this Call Bridge. You can prevent load balancing for empty conferences by using the parameter **`activeWhenEmpty`** set to **`false`** when performing the POST on the API object **`/calls`**.

2.5 Setting maximum quality levels for main video and content

This feature permits an administrator to specify a maximum resolution / frame rate pair for main video and/or for content using a callLegProfile. See the API commands in Section 2.11.2

Table 1 shows the settings available, and Table 2 explains the meanings of the settings.

Table 1: callLegProfile quality settings

Parameter	Value	Notes
qualityMain	**unrestricted** | max1080p30 | max720p30 | max480p30	For main video. Restricts the maximum negotiated main video call quality for this call leg based on limiting transcoding resources. Specified using a typical resolution and frame rate. Note that call legs may operate at lower resolutions or frame rates due to endpoint limitations or overall bridge load
qualityPresentation	**unrestricted** | max1080p30 | max720p5	For content. Restricts the maximum negotiated presentation video call quality for this call leg based on limiting transcoding resources. Specified using a typical resolution and frame rate. This only affects call legs which use a separate presentation stream.

Table 2: Description of maximum quality level settings

Setting	Description
unrestricted	Default, if setting not specified. Matches the behavior of older Call Bridge versions, where no restrictions are placed on resolution or frame rate.
max1080p30	Restricts the Call Bridge to negotiating at most 1920x1080 screen size at 30 frames per second (1080p30) or equivalent, for example 1280x720 screen size at 60 frames per second (720p60). Note: 720p60 is not a separate option, use the max1080p30 setting to allow 720p60.
max720p30	Restricts the Call Bridge to negotiating at most 1280x720 screen size at 30 frames per second or equivalent transcoding resources.
max480p30	Restricts the Call Bridge to negotiating at most 868x480 screen size at 30 frames per second or equivalent transcoding resources.

2.6 Improved DTMF comma handling

Prior to version 2.2, commas included in an API-specified **`dtmfSequence`** did not introduce any noticeable pause. In version 2.2, a two second pause has been introduced to make the pause noticeable.

Note: **`dtmfSequence`** is a string of DTMF characters that the Meeting Server sends to the far end either when the call leg initially connects, or during the call.

2.7 Layout and screen changes to improve user experience

The following layout and screen changes have been made to improve the user experience during meetings:

- the borders between participant panes have been removed, the panes now touch,
- in the overlay layout, the active speaker is now full screen,
- added the ability to remove the participant count icon on the screen,
- added the ability to use the importance level of participants to to control which participants are displayed onscreen.

2.7.1 Removing and showing the on-screen Participant Counter

Version 2.2 introduces a new **`participantCounter`** setting within **`callLegProfile`** objects; this allows you to control when the participant count value is shown on screen. Set **`participantCounter`** to one of the following values:

`auto`	shows the participant count value if there are off-screen participants; this is the default behavior and how the feature works in releases prior to 2.2
`never`	use this value to disable the participant count value so it is never included in Meeting Server video layouts
`always`	with this setting, the participant count value will be shown on screen permanently, even if there are no off-screen participants

For example, to disable the Participant Counter so that it is never shown, perform a PUT on the API object **`/callLegProfile/<call leg profile id>`** with parameter **`participantCounter`** set to **`never`**.

2.7.2 Using the importance level of participants to control which participants are displayed onscreen

Version 2.2 enables you to assign an importance level to participants in a conference. Multiple participants can be assigned different importance levels, the participant with the highest importance level will be treated as if they are the loudest speaker when determining whose video is shown on the screen.

For telepresence, stacked, speakerOnly and onePlusN screen layouts, the participant with the highest importance level will be shown in the main screen, rather than the active speaker; if there are multiple participants with the same highest importance level, then one of these will be shown in the main screen, which one being determined by who was the most recent active speaker. The Active speaker indication of a blue line below the speaker's video pane remains unaffected.

For the allEqual family of layouts, the participant with the highest importance level will be shown in one of the allEqual panes. If there are multiple important participants then up to 25 will be displayed in the allEqual panes, any remaining places will be taken by participants without importance set.

Initially, all participants have an unset importance level, any set importance level is higher than the unset state. An importance level of 1 is higher than 0, but lower than 2, and all these levels are higher than unset.

Example of using importance :

1. Remove any configured importance settings for all participants in the conference, so all participants are in the unset state.

   PUT to API object **`/calls/<call id>/participants/*`** with request parameter **`importance`** unset ("")

2. Add the important person to the conference with the importance level set.

   POST to API object **`/calls/<call id>/participants/`** with request parameter **`importance`** set, for example to 1.

3. To make a participant important if they are already in a conference:

   PUT to API object **`/participants/<participants id>/`** with request parameter **`importance`** set, for example to 1

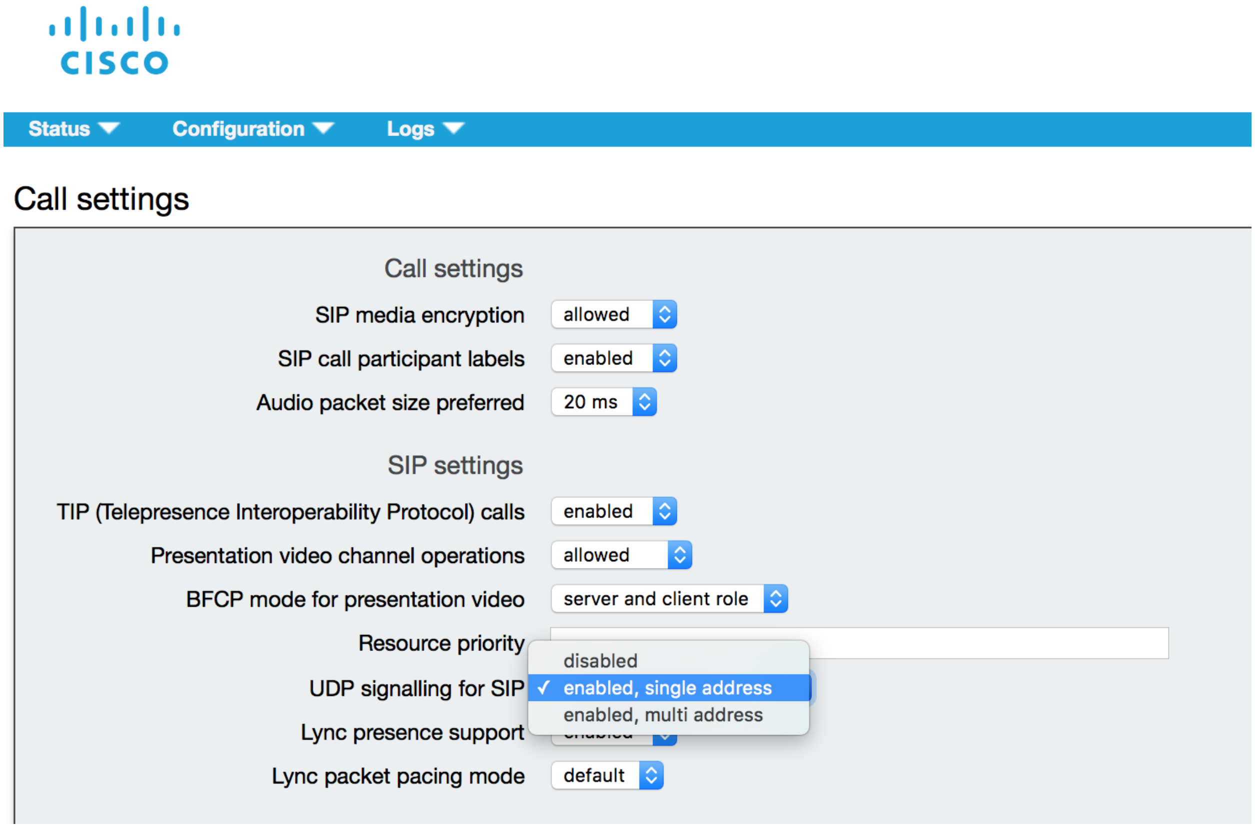
2.8 Enabling and disabling UDP signaling for SIP

The "UDP signaling for SIP" setting allows you to completely disable SIP over UDP, or to enable "single address" or "multi address" mode. Single address mode corresponds to the SIP over UDP behavior in versions prior to 2.2 and is the default, multi address mode allows SIP over UDP on multiple interfaces.

Use multi address mode if the Call Bridge is configured to listen on more than one interface for SIP over UDP traffic. Disable "UDP signaling for SIP" if you use SIP over TCP, or require that all of your network traffic is encrypted .

The "UDP signaling for SIP" mode is set through the Web Admin interface of the Call Bridge. Log into the Web Admin interface and select **Configuration>Call settings**, see Figure 1.

Figure 1: Settings for UDP signaling for SIP



Call settings

Call settings

SIP media encryption	allowed
SIP call participant labels	enabled
Audio packet size preferred	20 ms

SIP settings

TIP (Telepresence Interoperability Protocol) calls	enabled
Presentation video channel operations	allowed
BFCP mode for presentation video	server and client role
Resource priority	
UDP signalling for SIP	disabled ✓ enabled, single address enabled, multi address
Lync presence support	enabled
Lync packet pacing mode	default

2.9 Diagnostic tools to help Cisco Support troubleshoot issues

2.9.1 Log bundle

In version 2.2, the Meeting Server can produce a log bundle containing the configuration and state of various components in the Meeting Server. This log bundle will aid Cisco Support speed up their analysis of your issue.

If you need to contact Cisco support with an issue, follow these steps to download the log bundle from the Meeting Server.

1. Connect your SFTP client to the IP address of the MMP.
2. Log in using the credentials of an MMP admin user.
3. Copy the file logbundle.tar.gz to a local folder.
4. Rename the file, changing the logbundle part of the filename to identify which server produced the file. This is important in a multi-server deployment.
5. Send the renamed file to your Cisco Support contact for analysis.

2.9.2 Ability to generate a keyframe for a specific call leg

A new **`generateKeyframe`** object has been added to **`/callLegs/<call leg id>`**. POST to **`/callLegs/<call leg id>/generateKeyframe`** to trigger the generation of a new keyframe in outgoing video streams for the call leg in question. This is a debug facility, and Cisco Support may ask you to use the feature when diagnosing an issue.

2.9.3 Reporting registered media modules in syslog

From version 2.2, syslog will now print a message every 15 minutes to allow people to monitor whether all media modules are alive and well.

An example from an Acano X3 server:

```
Apr 21 09:53:50 user.info cms-emea-01 host: server: INFO : media module status
11111111111
```

2.10 Summary of MMP changes

Version 2.2 has no new MMP commands.

2.11 Summary of API Additions & Changes

New API functionality for the Meeting Server 2.2 includes support for:

- Office 365 Dual Homed Experience with OBTP Scheduling
- setting the maximum quality levels for main video and content
- load balancing of outbound calls to SIP endpoints
- diagnostics for recordings, streamings and Web Bridges
- enabling and disabling the on-screen participant counter

there are also some other miscellaneous additions.

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

2.11.1 Office 365 Dual Homed Experience with OBTP Scheduling

New request parameter added to **`/inboundDialPlanRules`** and **`/inboundDialPlanRules/<inbound dial plan rule ID>`**: **`resolveToLyncSimpleJoin`**

2.11.2 Setting the maximum quality levels for main video and content

New request parameters to **`/callLegProfile`** : **`qualityMain`**, **`qualityPresentation`**

2.11.3 Support for load balancing of outbound calls to SIP endpoints

New request parameter to **/callBridgeGroups**: **loadBalanceOutgoingCalls**

New request parameters to **/calls/<call id>/participants**: **callBridgeGroup**, **callBridge** for POST operations only

New request parameter to **/outboundDialPlanRules** and **/outboundDialPlanRules/<outbound dial plan rule id>**: **callBridgeGroup**

Added value to **scope** parameter for **/outboundDialPlanRules**: **callBridgeGroup**

New request parameter to **/calls**: **activeWhenEmpty**

2.11.4 Assigning an Importance level to participants to control the screen layout

New request parameter to **/calls/<call id>/participants/**: **importance** (POST only)

New request parameter to **/participants/<participant id>**: **importance** (PUT only)

NewAPI object: **/calls/<call id>/participants/*** with request parameter: **importance** (PUT only)

2.11.5 Retrieving diagnostics on a Recorder/Streamer/Web Bridge

New node added to **/recorders/<recorder id>**, **/streamers/<streamer id>**, **/webBridges/<web bridge id>**: **status**

2.11.6 Support to disable and re-enable the on-screen participant counter

New request parameter added to **/callLegProfiles**: **participantCounter**

2.11.7 Miscellaneous additions

- New request parameter added to **/coSpaces** and **/coSpaces/<coSpace ID>**: **meetingScheduler**
- New read-only field added to **/calls/<call ID>**: **ownerName**
- New request parameter added to **/system/status**: **cdrCorrelatorIndex**. This support external tools to the Meeting Server determining whether they have received all CDR records that have been sent.
- New operation to **/calls/<call id>/participants/*** with attributes **layout** or **(rx|tx)(Audio|Video)Mute**
- New request parameter added to **/compatibilityProfiles** and **/compatibilityProfiles/<compatibilityProfile ID>**: **sipMediaPayloadTypeMode**
- New object **/callLegs/<call leg id>/generateKeyframe**. POST to **/callLegs/<call leg id>/generateKeyframe** to trigger the generation of a new keyframe in outgoing video

streams for the call leg in question. This is a debug facility, and Cisco Support may ask you to use the feature when diagnosing an issue.

2.12 Summary of CDR Additions & Changes

Version 2.2 introduces the following changes to the Call Detail Records of the Meeting Server:

- ownerName field added to callStart records

The ownerName field is populated from one of the following (in priority order):

- meetingScheduler set through the API
- name field in /user corresponding to owner
- Jid field in /user corresponding to owner
- Not filled in if none of the above exist.

3 Notes on Installing and Upgrading to Cisco Meeting Server 2.2

If you have recently purchased a Cisco Meeting Server 2000, Cisco Meeting Server 1000 or Acano X-series server, the Meeting Server software is already installed, however a new version may have recently been released.

For the Cisco Meeting Server 2000 following the instructions in the installation guide to determine the version installed. For the Cisco Meeting Server 1000 or Acano X-series server, check the release using 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.

If your Meeting Server is running the latest software version then go to Section 3.2.

Note: This section assumes that if you are upgrading a Cisco Meeting Server 1000, an Acano X-Series server or specification-based VM that you are upgrading from 2.1.x. If you are upgrading from 2.0.x, then Cisco recommends that up you upgrade to 2.1.x first following the instructions in the 2.1.x release notes, before following any instructions in these Cisco Meeting Server 2.2 Release Notes.

Note: It is possible to upgrade from release 1.9.x to Cisco Meeting Server 2.2 without upgrading to 2.0.x and 2.1.x, however this has not been tested by Cisco.

3.1 Upgrading to Release 2.2

The instructions in this section apply to both Meeting Server and virtualized deployments with a previous Meeting Server release already installed and not clustered. Refer to the Scalability and Resilience Deployment Guide before upgrading clustered servers.

CAUTION: Before upgrading to release 2.2.2 you must 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. Do NOT use the automatic backup file that is created during the upgrade process.

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.

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

1. Obtain the appropriate upgrade file from the support section of the Cisco website. There will be five files:

   Cisco_Meeting_Server_2_2_2_CMS2000.zip

   This file requires unzipping to a single upgrade.img file. Use this file to upgrade Cisco Meeting Server 2000 servers, follow the instructions below.

   Cisco_Meeting_Server_2_2_2_vm-upgrade.zip

   This file requires unzipping to a single upgrade.img file. Use this file to upgrade vm deployments, follow the instructions below.

   Cisco_Meeting_Server_2_2_2.vhd

   Use this file to upgrade Microsoft Hyper-V deployments

   Cisco_Meeting_Server_2_2_2_x-series.zip

   This file requires unzipping to a single upgrade.img file. Use this file to upgrade Acano X-series servers, follow the instructions below.

   Cisco_Meeting_Server_2_2_2.ova

   Use this file for new vm deployments, follow the steps in the Installation Guide for Virtualized Deployments.

   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.

2. Validate the download; the checksums for the 2.2.2 release are shown in a pop up box that appears when you hover over the description for the download.
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:
   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.
   c) After copying the upgrade.img file, you will not be able to see it listed as being in the file system; this is normal.

4. Copy the software to the Server/ virtualized server.
5. To apply the upgrade, issue the upgrade command.

   a. Establish a SSH connection to the MMP and log in.
   b. Initiate the upgrade by executing the upgrade command.

      ```
      upgrade
      ```

      The Server/ virtualized server restarts automatically: allow 10 minutes for the process to complete.

6. Verify that the Meeting Server is running the upgraded image by re-establishing the SSH connection to the MMP and typing:

   ```
   version
   ```

7. Check the **Configuration > Outbound Calls** rules updating the Local Contact Domain field and completing the new Local From Domain field if necessary.
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 Cisco Meeting Server 2.2 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.

3.2.1 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.

3.2.2 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.

3.2.3 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.

3.3 Downgrading

To return to the previous version of the server software in a non-clustered environment, use the regular upgrade procedure to "upgrade" to the appropriate version. Then restore the configuration backup for the older version, using the `backup rollback <name>` command. See the MMP Command Reference document for full details. Do not rely on the backup generated automatically during upgrade.

Note: The `backup rollback <name>` 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.

4 Bug search tool and 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 `2.2.0`.
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 2.2.2

Cisco identifier	Summary
CSCve70685	Occasionally, the Cisco Meeting Server restarts when a participant is put on hold and then activated.
CSCve65931	Multiple Call Bridges configured as a group may cause the Cisco Meeting Server to restart during PIN entry.
CSCve39382	With a Call Bridge group setup, the caller ID displayed on the calling endpoint can be inconsistent depending upon whether a call has been replaced or not.
CSCve31915	In dual homed meetings involving a cluster of Call Bridges, if a Lync participant locks the spotlight on itself, participants on a remote Call Bridge will only see participants on that Call Bridge, rather than the Lync participant as expected.

Cisco identifier	Summary
CSCve70201	Audio quality significantly degrades during very high load. This may happen during peak hours when hundreds/thousands of audio and video calls as well as hundreds of distributed links are being hosted on a Meeting Server.
CSCve28532	In dual-homed S4B/Lync meetings hosted on clustered Meeting Servers, participants using XMPP clients, i.e. web clients or the Cisco Meeting App, will not see the presentation if the client is connected to a different core server in the clustered deployment to the one that has the call to the AVMCU conference.
CSCve22901	If a member is logged into the Cisco Meeting App and observing their space when a participant calls into the space, sometimes the member sees the name of the new participant appear in green under the space name, but not always.
CSCve21895	Frozen video from S4B clients in a dual-homed conference is sent to SIP endpoints. This occurs from S4B client version 16.0.7766.5299.
CSCve18884	In some rare circumstances, dropped video frames and throttling occurs in video sent from a Meeting Server, even when the unit is not heavily loaded.
CSCve18504	When a Lync conversation is escalated to a Lync meeting, any subsequent SIP endpoints (added to this meeting via an SFB client), will incorrectly see the first SIP endpoint's address in the FROM field of the incoming SIP INVITE (instead of the SFB client). This is only an issue if the SIP endpoint is specifically looking at the incoming caller ID; once connected to the Lync meeting, all participants' names are correctly shown on their respective video stream

Issues seen in previous versions that are fixed in 2.2.1

Cisco identifier	Summary
CSCve35795	Office 365 Dual Homed Experience with OBTP Scheduling (also known as Lync simplejoin) doesn't work with newer server releases of Office 365 and fails with the message "lync simplejoin resolution: resolution failed (conference not found)" even though the O365 meeting does exist.
CSCve22765	Inconsistent voice prompts played to users when Call Bridge group is used.
CSCve20873	Guests can join via a hyperlink even when guest access via hyperlink is set to disabled.
CSCve18410	French translations for Web Bridge guest join options require improvement.

Issues seen in previous versions that are fixed in 2.2.0

Cisco identifier	Summary
CSCve26277	Cisco Meeting Server doesn't respond to BFCPHello from HDX when BFCP mode is “server and client”.
CSCve26267	Directory search does not search on ‘first name’ field
CSCve08053	Choppy mpeg4-generic encrypted audio from TelePresence Server.

4.2 Open issues

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

Cisco identifier	Summary
CSCve64225	Cisco UCS Manager for Cisco Meeting Server 2000 should be updated to 3.1(3a) to fix OpenSSL CVE issues.
CSCve60309	Cisco UCS Manager 3.1(3a) reports 'DIMM A1 on server 1/1 has an invalid FRU' as the CMS 2000 DIMMs are not listed in the 3.1(3a)T catalog.
CSCve37087 but related to CSCvd91302	One of the media blades of the Cisco Meeting Server 2000 occassionally fails to boot correctly. Workaround: Reboot the Fabric Interconnect modules.
CSCve26287	TIP endpoint doesn't display video when quality is below 720p.

Cisco Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

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

Cisco Trademark