Cisco Meeting Server

Cisco Meeting Server Release 2.2.14

Release Notes

December 13, 2018

Contents

What's changed

Version	Change
2.2.14	Added section Resolved in 2.2.14. Hashes updated.
2.2.13	Added section for new interactive API reference tool.(Sept 24, 2018)
2.2.13	Open issues updated. Load balancing note updated. (Sept 03, 2018)
2.2.13	Support for Cisco Meeting Server 2000 added–hashes updated. Open Issues updated.
2.2.13	Added section "Resolved in 2.2.13"
2.2.12	Minor correction to unset the importance parameter on /calls/<call id>/-participants/*
2.2.12	Added section "Resolved in 2.2.12"
2.2.11	Added section "Resolved in 2.2.11"
2.2.10	Added section "Resolved in 2.2.10", and added note about running this build on your Meeting Server before upgrading to 2.3.x
2.2.9	Added section "Resolved in 2.2.9"
2.2.8	Added section "Resolved in 2.2.8"
2.2.7	Added section "Resolved in 2.2.7"
2.2.6	Added section "Resolved in 2.2.6"
2.2.5	Added section "Resolved in 2.2.5"
2.2.4	Added section "Resolved in 2.2.4"
2.2.3	Added section "Resolved in 2.2.3". Added section on "Enhanced support for dual screen endpoints"
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 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: From version X8.9, the Cisco Expressway supports traversal of SIP traffic at the edge of the network, to and from the Meeting Server; we recommend upgrading to the latest version of the Cisco Expressway software. You are advised 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 a future version of the Cisco Meeting Server software.

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

Note 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. From version 2.3 of the Meeting Server software, there will be no further development or feature releases related to the H.323 Gateway component, and in version 2.5 the component will be removed from the Meeting Server software. Customers are encouraged to start evaluation of the more mature H.323

Gateway component in the Cisco Expressway, and plan their migration over.
Any H.323 endpoints registered to Expressway-E or Expressway-C will not consume Rich Media Session (RMS) licenses when calling into the Cisco Meeting Server from Expressway version X8.10 onwards.

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 incoming calls: From Meeting Server version 2.1, there is a change to the way the Cisco Meeting App handles incoming calls. By default incoming calls are not allowed. To allow incoming calls to Cisco Meeting App users, set parameter **`canReceiveCalls=true`** for API object **`/user/profiles/<user profile id>`**.

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

- the capability to determine whether to display security icons on endpoints
- support for Office 365 dual homed experience with OBTP scheduling
- enhanced support for dual screen endpoints
- 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.

There is also a new interactive API reference tool enabling you to see a high level view of the API objects and drill down to lower levels for the detail, see here for more information.

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 TURN Server, 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 1.1. 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 Bridges 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 Enhanced support for dual screen endpoints

From version 2.2.3, the Meeting Server supports showing video across both screens of a dual screen endpoint running CE9.1.1 (or later), in local calls within a Cisco Unified Communications Manager 11.5 deployment and calls over Cisco Expressway (X8.9).

When content is being shared with a dual screen endpoint, either one video and one content stream is sent, or in the case of a dual screen endpoint with a 3rd monitor connected, two video streams and one content stream are sent.

All layouts that are supported in ActiveControl are supported in dual screen endpoint mode, where:

- **single** (also known as speakerOnly) has the two most active speakers full screen, one on each screen.
- **overlay** (also known as telepresence) has the two active speakers in full screen, and up to 12 pips overlayed at the bottom of the two screens.
- **1plusN** (also known as Prominent) has the active speaker full screen on the left endpoint and the right endpoint has an NxN layout which grows automatically up to 3x3.
- **equal** (also known as allEqual) has participants evenly distributed between the left and right screen with up to two 3x3 grids on both screens.

The default layout is the existing prevailing layout applied to the callLegProfile or space.

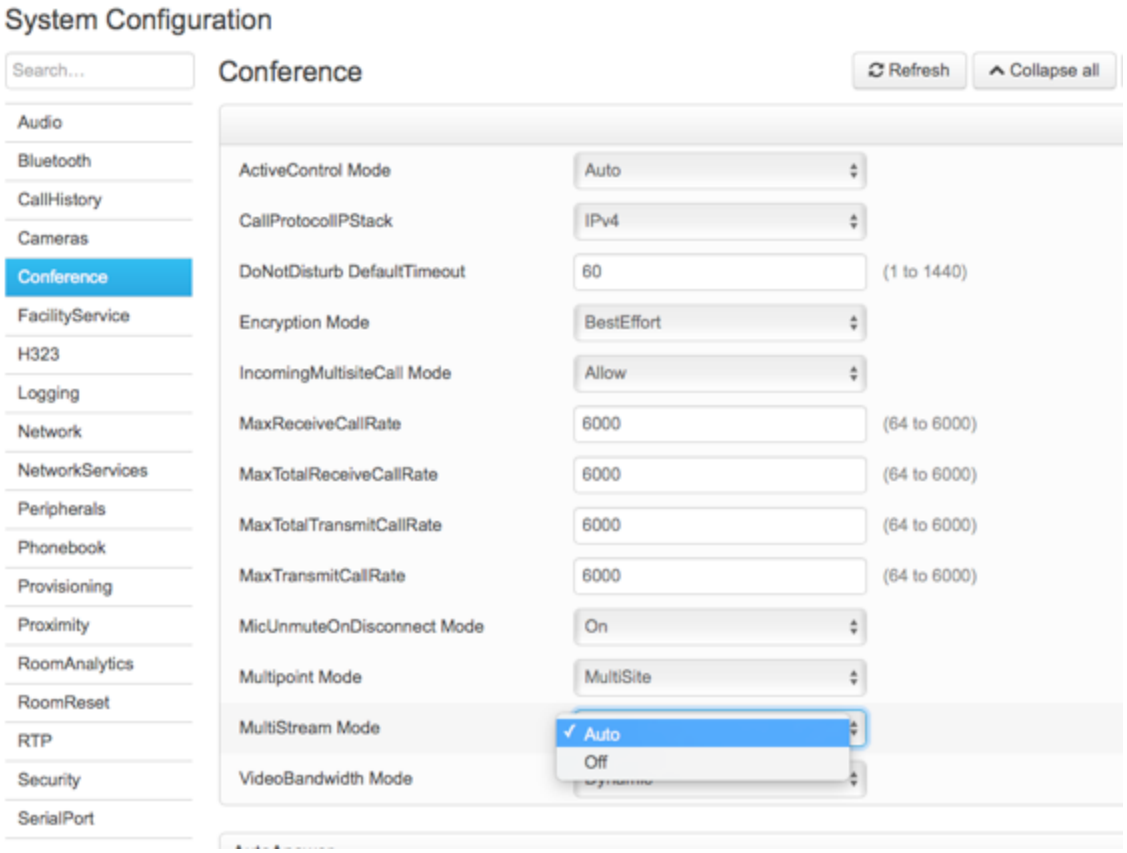
2.4.1 Enabling dual screen endpoint support

Support for dual screen endpoints is disabled by default. To enable support:

1. POST to **`/compatibilityProfiles`** or PUT to **`/compatibilityProfiles/<compatibility profile id>`** the parameter **`sipMultistream`** set to true.
2. Add the compatibilityProfile to the system profile. PUT the **`compatibilityProfile`** parameter and **`ID`** to **`/system/profiles`**.

3. In addition to the Meeting Server configuration, the dual screen endpoints also require configuration. On the web interface of the endpoint, navigate to **`Setup>Conference`** and select **`Multistream mode`**.

Table 1: Configuring Multistream mode on the endpoint



Note: Endpoints that support ActiveControl render participant count and the recorder indicator locally on the endpoints and touch panels. Endpoints not supporting ActiveControl will have the labels and indicators sent from the Meeting Server to one of the endpoints.

2.4.2 Disabling dual screen endpoint support

To re-disable dual screen endpoint support after enabling it:

1. Identify the compatibilityProfile that is applied to **`/system/profiles`** with **`sipMultistream`** set to true.
2. PUT to **`/compatibilityProfiles/<compatibility profile id>`** the parameter **`sipMultistream`** set to false, where **`<compatibility profile id>`** is the ID of the compatibilityProfile identified in step 1.

2.5 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 examples 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 or to Cisco Meeting App is not currently supported by Call Bridge Groups.

2.5.1 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.

2.5.2 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.

2.5.3 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.

2.5.4 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 the load balancing preferentially using the empty conferences, by setting the parameter **activeWhenEmpty** to **false** when performing the POST on the API object **/calls**.

2.6 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 2.12.2

Table 2 shows the settings available, and Table 3 explains the meanings of the settings.

Table 2: 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 3: 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.

2.7 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.

2.8 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.

2.8.1 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`**.

2.8.2 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 (leave parameter value blank)

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

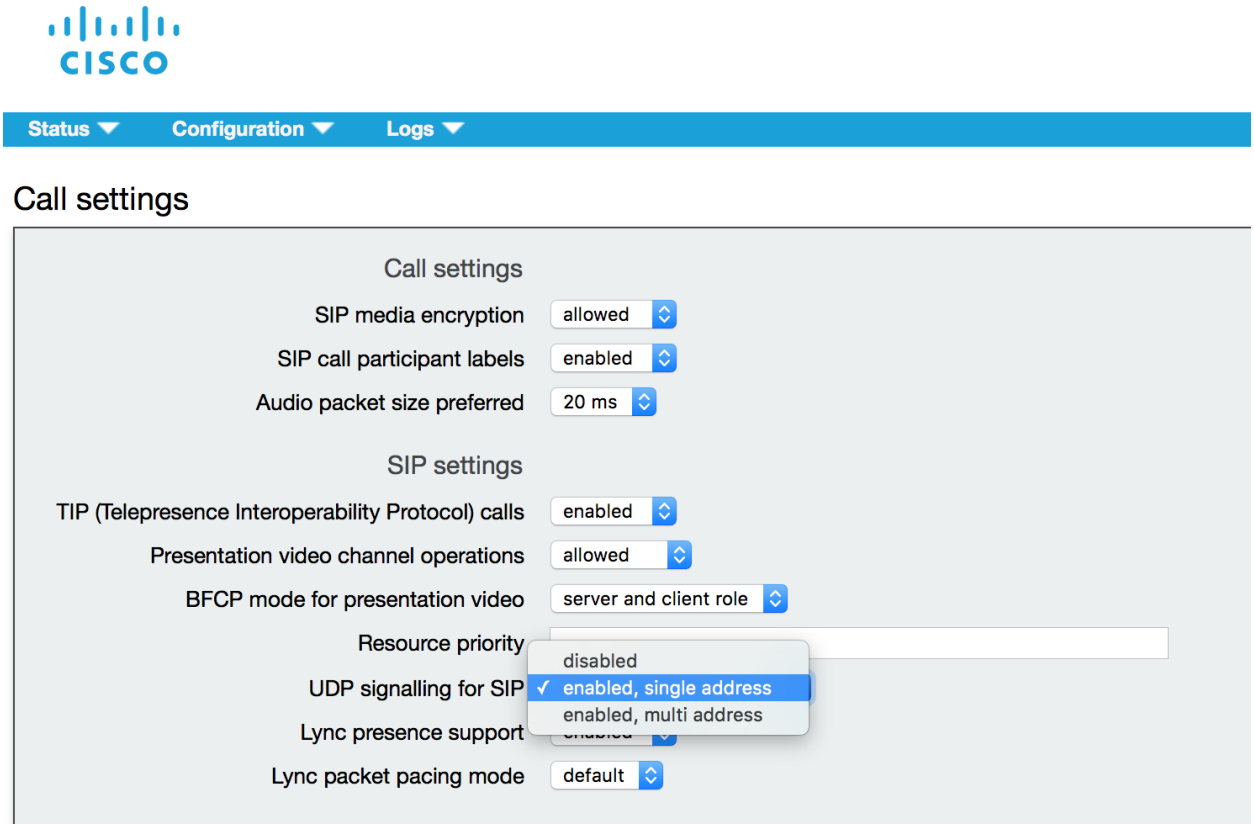
2.9 Enabling and disabling UDP signaling for SIP

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



2.10 Diagnostic tools to help Cisco Support troubleshoot issues

2.10.1 Log bundle

From 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. It will include some of the following files:

- syslog
- live.json
- dumps
- db

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.

Initial file size of the log bundle.tar.gz is 1 Kb, after transfer via SFTP the size will increase depending on the number of files and their size.

2.10.2 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.

2.10.3 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
```

2.11 Summary of MMP changes

Version 2.2 has no new MMP commands.

2.12 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
- an enhanced experience on dual screen endpoints
- 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.

2.12.1 Office 365 Dual Homed Experience with OBTP Scheduling

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

2.12.2 Setting the maximum quality levels for main video and content

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

2.12.3 Additional support for Dual Video Endpoints

New request parameter to **/compatibilityProfiles** and **/compatibilityProfiles/<compatibility profile id>**: **sipMultistream**

2.12.4 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**

2.12.5 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)

2.12.6 Retrieving diagnostics on a Recorder/Streamer/Web Bridge

New node added to **/recorders/<recorder id>**: **activeRecordings**

New node added to **/streamers/<streamer id>**: **activeStreams**

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

The table below shows the status settings for the components.

Status	Component	Recorder	Streamer	Web Bridge
unused	component is unused	✓	✓	✓
success	connected to the queried Call Bridge	✓	✓	✓
connectionFailure	could not connect to the queried Call Bridge	✓	✓	✓
invalidAddress	the configured URL is invalid	✓	✓	
dnsFailure	the configured URLcannot be resolved by the DNS server	✓	✓	
remoteFailure	a connection was established with the component but the Call Bridge received a failure response	✓	✓	
unknownFailure	an unknown failure occured	✓	✓	
lowDiskSpace	has limited disk space available	✓		

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

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

2.12.8 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.

2.13 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.

2.14 New interactive API reference tool

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

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

Steps to use the tool:

1. Click **View the docs**
2. Select a category from the list in the left pane. For example: Call Related Methods.
3. Click on any method to see URI: GET/POST/PUT. Refer to the table of parameters and response elements with descriptions. For example: GET https://ciscocms.docs.apiary.io/api/v1/calls?

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

Learning labs

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

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

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

3 Upgrading, downgrading and deploying Cisco Meeting Server software version 2.2

This section assumes that you are upgrading from Cisco Meeting Server software version 2.1. If you are upgrading from an earlier version, then Cisco recommends that you upgrade to 2.1 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: Cisco has not tested upgrading from a software release earlier than 2.1.

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 2.2

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 to release 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_14_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_14_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_14.vhd

Use this file to upgrade Microsoft Hyper-V deployments

Cisco_Meeting_Server_2_2_14_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_14.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 2.2.14 release are 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-256 hash values in the table below.

Type	File	Hash
Server (X Series)	upgrade.img	4a6909697424ad52133a591efed912ce12abe8f7be73ea9845bc57f1c1aab9ea
CMS 2000	upgrade.img	6e320b9ea8f991d23fea6fd9cefa15ff632c24b04b35b771221bf6a1dad6d946
VM	Cisco_ Meeting_ Server_2_2_ 14.ova	4ac91588a29a136a4776902dd797377412804dc40b038d92f5f7f21370fe677a
VM	Cisco_ Meeting_ Server_2_2_ 14.vhd	3dd0c90a9fec34b24f84801898ff2f24c26b430cfcf5d15d0f938da49631d0c5
VM	upgrade.img	e79bba84454fa9205c1ce7ee35c487726ca88a5050acfb8906a742fa7fba601d

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.
   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 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 in the table 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. Check the **Configuration > Outbound Calls** rules updating the Local Contact Domain field and completing the new Local From Domain field if necessary.
9. Update the customization archive file when available.
10. 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.

11. 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.
12. You have completed the upgrade.

Note: If you have a Cisco Expressway connected to the Meeting Server then ensure that you run this version on your Meeting Server for at least seven days. This is required to resolve the cache issue which prevented the Meeting Server WebRTC from working with Cisco Expressway.

3.2 Downgrading

If anything unexpected occurs during the upgrade process you can return to the previous version of the server software.

Use the regular upgrade procedure to "upgrade" the Meeting Server to the appropriate version. Then restore the configuration backup for the older version, using the MMP command **`backup rollback <name>`** command. Do not rely on the backup generated automatically during upgrade. For deployments with clustered databases read the instructions in this FAQ, before "upgrading" clustered servers.

Note: In some rare cases with clustered deployments, it might be necessary to do the **`factory_reset app`** procedure on each server. For more information, see https://kb.acano.com/content/5/250/en/how-do-i-upgrade-a-resilient-deployment.html

---

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.

3.3 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.

3.3.1 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 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 `2.2.14`.
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 2.2.14

Cisco identifier	Summary
CSCvm95156	When running a trunk debug on Cisco Meeting Server 2000, it returns an error that the file is not found.
CSCvn58291	Chrome Version 71 not working with Cisco Meeting Server 2.2.x therefore users are unable to join calls.
CSCvm73261	An unexpected restart after call failures can occur.
CSCvk76283	Streamer play from Vbrick using HLS may stop streaming and report an error that "play-back of this video is not available, please try again later" .
CSCvi48985	In rare circumstances, a Cisco Meeting Server may stop sending video for some calls.
CSCvk12210	Syslog and audit log files on Cisco Meeting Server 2000 may unexpectedly become truncated below their expected 100MB file maximum.

Cisco identifier	Summary
CSCvk01492	Some log files created on X-series Meeting Server are empty. Meeting Server fails to write logs in the syslog and produces a write error message.
CSCvj98031	Skype for Business client intermittently does not display content when sharing from SIP endpoint.
CSCvj65137	Lync SimpleJoin request may get forwarded to forwarding rules or have a connection problem during resolution of the web link.
CSCvj63727	Attempt to send packets after a call has ended can lead to media framework restart.
CSCvn00962	Occasionally recording loses lip sync and does not recover.
CSCvi89736	Meeting Server streamer integration with Adobe Media Server 5.0.15 fails due to the Adobe Media Server rejecting the connection request because of a mismatch on the application string sent by Meeting Server streamer.
CSCvg64570	In rare circumstances Cisco Meeting Server may unexpectedly reboot whilst processing a webadmin or API command.
CSCve08058	Load balancers stop working after a network issue. After disabling and re-enabling the load balancers start working again.
CSCvk77779	CDR receiver cannot receive CDR messages from Cisco Meeting Server.

Issues seen in previous versions that are fixed in 2.2.13

Cisco identifier	Summary
CSCvj43978	The Call Bridge can restart while trying to print an invalid log message.
CSCvj83274	Meeting Server does not respond to NOTIFY for participant removed from S4B Enterprise pool.
CSCvi94545	Inter-call bridge traffic not correctly QoS tagged.
CSCvi82708	Video to streaming client will drop to 352x288 and low fps when no main video is incoming to a Meeting Server conference and presentation is being shared.
CSCvi71986	In rare circumstances the Web Bridge may restart unexpectedly during a call.
CSCvi61556	Low FPS to streaming client.
CSCvi54717	Using API, doing POST to Calls with **`messageText`**, **`messagePosition`**, and **`messageDuration`** does not work on the clustered Meeting Server.
CSCvj93516	A high rate of syslog messages related to database clustering can be emitted from a Meeting Server running on Meeting Server 2000 that is part of a database cluster.
CSCvi93240	H323 Gateway can restart causing all calls to drop.
CSCvf40213	Advertisement of multiparty capability in TIP.

Cisco identifier	Summary
CSCvi25591	A crash dump is created following a database cluster creation. There is no impact as the Call Bridge component is expected to restart at db cluster creation, which it does cleanly after the crash.

Issues seen in previous versions that are fixed in 2.2.12

Cisco identifier	Summary
CSCvi31989	Audio and video calls are broken with Lync when using Lync Edge.
CSCvh95331	The Call Bridge component on a Meeting Server may unexpectedly restart after processing a large number of calls. This will lead to a drop of all calls connected to this one Call Bridge. The Call Bridge should be able to process new calls within a few seconds of the restart.

Issues seen in previous versions that are fixed in 2.2.11

Cisco identifier	Summary
CSCvh82567	Meeting Server Module 0 crashes when looking up a call/conference GUID for a message that can't be resolved.
CSCvh92980	Spuriously high round trip times for audio and video may be reported by Meeting Server for Lync/Skype for Business calls. This does not appear to affect audio or video quality.
CSCvh71270	Lync/Skype for Business client desktop shares fail when media encryption is set to "Required" on Meeting Server.
CSCvh67644	Some third party endpoints and SIP servers can result in SIP calls via Cisco Unified Communications Manager disconnecting 15 minutes after call setup.
CSCvh84453	Meeting Server does not reply to NOTIFY of Lync/Skype Focus call in dual home meeting. Consequently the Focus call is not disconnected from the Lync/Skype side and therefore new dual home calls are unable to connect.
CSCvg78320	When WebRTC client starts/stops content, media sometimes fails in both directions.
CSCvg25105	Office 365 dual home calls experience one way video when using VCS Expressway TURN.
CSCvg22680	In some circumstances H.323 Gateway doesn't handle incoming SIP calls from the Call Bridge. After 40 seconds, the call fails with the message "timeout - provisional response".
CSCvg22663	H.323 Gateway stops accepting calls with the message "reached call limit" after 100x "busy" calls. In this situation, no incoming/outgoing H.323 calls can be made on Meeting Server even if there's no ongoing H.323 call.

Issues seen in previous versions that are fixed in 2.2.10

Cisco identifier	Summary
CSCvh66298	In Cisco Unified Communications Manager/Cisco Meeting Server deployments, ad hoc call escalation may fail from lack of resources if remote teardown occurs before the local teardown, resulting in spaces not being returned to the pool.
CSCvh66295	Meeting Server sends lower bandwith to SIP endpoints than configured.
CSCvh49823	Video from the Meeting Server displayed on SIP endpoints appears to jump or twitch.
CSCvh31022	Using Cisco Meeting App 1.10 for desktop or WebRTC and selecting the option “Use my phone” to call a number, results in a dial transform not being applied to the out-bound call.
CSCvh21861	Meeting Server may crash with error message " server-!ServerManagementCmgrClientInstance::PasscodeResolverUser_handlePasscodeRes-olutionFailure [server_management_cmgr_client_instance.cpp : 186 + 0x7]" .
CSCvh21225	The Meeting Server may crash with error message “server crash : server-!SfNetworkDataPort” if using the TURN server.
CSCvh21118	Meeting Server may reboot in Lync deployments when under high load and calls are load-balanced, the Lync friendly display name label is lost or delayed and the Lync call URI is longer than 56 bytes.
CSCvh10994	Some display names with long UTF-8 encodings are incorrectly truncated by the Meet-ing Server mid way through a character. These malformed SIP headers can result in call failures for devices that are strict on the format, for example Skype for Business.
CSCvh03762	In Cisco Unified Communications Manager/Cisco Meeting Server deployments, the Cisco IP Phone 9971 sends low quality video in ad hoc calls hosted on the Meeting Server.
CSCvg92785	The Call Bridge may restart when a SIP participant is disconnected from a meeting using Active Control.
CSCvg66561	Meeting Server may crash with error message “server!watchdog_thread_fn [main.cpp : 5538 + 0x0]” following invalid user authentication.
CSCvg54892	A recording started by an endpoint on one clustered Call Bridge cannot be stopped by an endpoint on another Call Bridge in the same cluster.
CSCvg42618	Under rare circumstances, the Meeting Server can unexpectedly restart after a SIP par-ticipant has joined a conference.
CSCvg39964	In a scheduled meeting Cisco TMS tells the Meeting Server to dial out to SIP endpoints registered to Cisco Unified Communications Manager. The participant is connected to the conference, but for some endpoint configurations the Meeting Server tells Cisco TMS that the participant is not connected, causing Cisco TMS to request a redial of the endpoint.
CSCvg21969	If the passcode has not been configured in a space, then intermittently the Call Bridge is unable to play the " you are the first participant" audio prompt.

Cisco identifier	Summary
CSCvf79666	After significant uptime, the Meeting Server drops the IVR timeout to about 10 seconds, rather than a minute.
CSCve08141	Meeting Server's media process may restart with error message "sf_assert failed common/include/sf_lock.h:122"
CSCvh24431	A cache issue prevents the Meeting Server WebRTC from working with Cisco Expressway.

Issues seen in previous versions that are fixed in 2.2.9

Cisco identifier	Summary
CSCvg58125	Lync simplejoin did not work if the user whose meeting you are trying to join has an apostrophe in their name.
CSCvg31108	Under certain circumstances, resolving multiple lync conference ids in rapid succession could result in the Call Bridge crashing.
CSCvg23980	After using the **`xmpp cluster status`** command, the XMPP server restarted followed by the Call Bridges being unable to reconnect.
CSCvg23896	Occasionally, participants are disconnected from TMS scheduled conferences.
CSCvg23720	In Expressway deployments with the Meeting Server, it is possible that federated Office 365 calls will drop after approximately 30 minutes. Ongoing local Meeting Server calls will continue, but all S4B participants will appear to be disconnected.
CSCvg41087	A media module on the Meeting Server, crashed with 'mf_remote_media!mf_pipe_source_run' message. Note: that this restart will not be observed by any users, as media module restarts do not affect users.
CSCvg41083	Call Bridge restarted due to Cisco Meeting App 1.10 pairing a call.
CSCvg23794	Desktop sharing fails when the Meeting Server is used as a gateway with Expressway TURN between Lync and SIP participants.
CSCvf78852	In some virtual dual NIC environments, reducing the MTU of any non-default interface to 1280 or lower results in a loss of network connectivity.
CSCve39303	On heavily loaded Meeting Servers, video freezes for Lync/Skype for Business calls, two to four minutes after they join the call.
CSCvg49776	Using the WebRTC 1.9 app in Finnish, username is incorrectly spelt as " Käyttääjnimi" .
CSCve14298	Using the WebRTC 1.9 app in Finnish, the " Sign in" button was incorrectly labelled as " Liity" .

Issues seen in previous versions that are fixed in 2.2.8

Cisco identifier	Summary
CSCvg01532	Attempting to change the layout for all participants in a call by using an API PUT to `/api/v1/<call id>/participants/*` may not work for all participants.
CSCvf99765	The Call Bridge unexpectedly crashes when a user dials into an IVR and twice enters the ID to a space without a passcode.
CSCvf89954	Unable to access the Web Admin Interface after upgrading to 2.2.7. This can happen if the same filenames have been used for the Web Admin Interface certificate and key over several software versions.
CSCvf87952	After many hundreds of thousands of calls, the Meeting Server can get into a state where it will stop sending RTCP packets to SIP participants. This can sometimes result in video not being decoded from these participants.
CSCvf84935	Occasionally, the Meeting Server may restart after some calls are put on hold.
CSCvf83879	The Web Admin doesn't start if it is using the admin interface on X series servers and a DER encoded certificate is applied.
CSCvf61515	Cisco Meeting Server 2000 is unable to initiate or join an XMPP cluster.
CSCvf42960	When the Meeting Server recorder is invoked for an audio only call, and no video is in the call, audio will be garbled and inaudible. The recording file will also be shorter than expected.
CSCvf39749	When a participant disconnects, in rare circumstances it is not correctly removed from the conference active speaker entry list, this list can then become invalid and cause the Meeting Server to unexpectedly restart.
CSCvf30323	Very large LDAP sync operations may fail with postgres errors in the Meeting Server syslog.
CSCve66586	After a while the recorder may stop creating video recordings on the NFS, even though the NFS location is not full.
CSCve29461	Error messages are unhelpful when the Meeting Server recorder is unable to write to the configured NFS share.

Issues seen in previous versions that are fixed in 2.2.7

Cisco identifier	Summary
CSCvf77597	Calls from a Cisco TelePresence System 3000 series may disconnect when using the Call Bridge Groups feature on the Meeting Server. One of the bandwidth parameters included in the SDP was incorrectly calculated, leading to the occasional call failing. For example, outbound calls to Cisco TIP systems may disconnect when using the Call Bridge Groups feature.

Cisco identifier	Summary
CSCvf77262 and CSCvf32293	For ActiveControl enabled endpoints, the Meeting Server will use the display name from the SIP remote-party-ID or Contact header (if available) in the participant list for an incoming call to a space, but for outbound calls only the SIP To: URI will be used for the name, and no Display Name will be used.
CSCvf76660	In rare cases, a participant is not always seen across a single distributed link in a cluster of Call Bridges.
CSCvf44130	When dialing two endpoints via the H.323 Gateway to the Call Bridge and one endpoint tries to present, the other endpoint receives content in the main video.

Issues seen in previous versions that are fixed in 2.2.6

Cisco identifier	Summary
CSCvf65214	When a Cisco Meeting App user dials a space which has multiple access methods, the Meeting Server will always present a prompt indicating they must enter a passcode, even if one is not required. An alternative prompt has been added “enter passcode (if required)”.
CSCvf51295	Some error messages in WebRTC calls may be incorrectly displayed in English when using the Japanese language pack.
CSCvf42693	Attempting to resolve a blank call ID for a Lync conference could cause the Meeting Server to restart.
CSCvf36654	In some call flows through a Cisco Unified Communications Manager, calls placed on hold to a Meeting Server may be disconnected after a period of time.
CSCvf36154	During some database to Call Bridge syncs, an unnecessarily large number of records may be updated, possibly reducing performance on heavily loaded systems or preventing some data from being updated.
CSCvf30053	In a clustered Meeting Server deployment, it is possible that TMS scheduled meetings will start late or have incorrect information, for example meeting names.
CSCve08594	After a period of time, an H.323 GW can stop accepting new calls. A restart of the H.323 GW fixes this problem. This problem could occur if the TCP channel for the H.245 connection for a particular H.323 call had closed.

Issues seen in previous versions that are fixed in 2.2.5

Cisco identifier	Summary
CSCvf31964	In some scenarios, some SIP endpoints may not be visible to any of the other participants in a conference.

Cisco identifier	Summary
CSCve86049	Presentation sharing may not be possible when multiple H.323 endpoints connect to a Meeting Server through the built-in H.323 Gateway.
CSCve35060	H.323 Gateway calls through an IVR will be disconnected if the Meeting Server setting for encryption is “Allowed”, but encryption is “Required” for the space.
CSCvf31494	In AVMCU meetings, SIP endpoints could have an avatar displayed rather than their own video, if media is encrypted between the AVMCU and the Meeting Server and the spotlight is locked on any participant for 15 minutes or longer. On unlocking, the SIP endpoint could be displayed as an avatar.

Issues seen in previous versions that are fixed in 2.2.4

Cisco identifier	Summary
CSCvf21142	Presentation video does not work between Meeting Server 2.2 and Polycom HDX endpoints.
CSCvf21169	If a tenant participant limit is specified, participants may not be admitted to a distributed call even if the limit has not been reached.
CSCvf14323	If a customized background image is in use, the background image is repeatedly loaded when lots of participants in a space need to be activated or deactivated en masse (for instance because a host joins a space with lots of guest users). If this background image file is fairly large, it causes an extra load on the system, which can eventually lead to a restart of the Meeting Server.
CSCvf09283	Under certain circumstances, connections from Lync to a clustered Meeting Server commence with a NEGOTIATE message with a To: URI of the following form: To: sip:<DN of pool>;ms-fe=<FQDN of CMS>. Currently, the Meeting Server uses the NEGOTIATE To: URI (minus any parameters) as its contact domain when responding to subsequent requests on that connection. Where present, the value of the ms-fe parameter would be a better choice, as it resolves to the individual Call Bridge rather than each / any of the Call Bridges in the pool.
CSCvf02256	callLeg API reports empty /alarms node with no further information as to what the alarms are.
CSCve84209	Reconnecting a WebRTC host participant doesn’t activate a SIP guest user.
CSCve49642	If a new distributed peer link is established 'after' a permanent messageText has been sent for a particular call, participants over the distributed link are not shown this message.

Cisco identifier	Summary
CSCvf21193	If custom branding resources (call branding or IVR branding) should be used for a call leg and the web server hosting these resources is unavailable, then the Meeting Server will wait for up to two minutes for a TCP response on every call leg in the conference before giving up and joining the endpoint to the conference. After this bug fix, the Meeting Server will delay the first call that needs custom branding resources for a short time before determining that they are not available, and proceeding without them. Subsequent calls will not be delayed.

Issues seen in previous versions that are fixed in 2.2.3

Cisco identifier	Summary
CSCve99788	The Call Bridge could crash in some circumstances while processing a request from a Lync client to add a SIP endpoint or Cisco Meeting App user to an AVMCU.
CSCve98059	Setting the date on a Cisco Meeting Server 2000 via the MMP only persists until reboot.The MMP should not offer the option to set the date. Set the date and time correctly in UCS Manager.
CSCve98053	The default hostname of a Cisco Meeting Server 2000 is “acano”, when it should be CMS2000.
CSCve87518	Participant name labels are missing in layouts with PIPs, for example stacked layout.
CSCve83819	When Lync proxy connections are used in a clustered deployment of Meeting Servers, content sharing in a dual-homed call to a Lync or S4B client shows a black screen.
CSCve72610	Chat messages do not appear in the chat window for a non-member user connected to a space. This occurs when the /callProfile has parameter “messageBoardEnabled” initially set to false, but is subsequently changed to true.
CSCve68664	H.323 Gateway restarts unexpectedly with h323 process: signalled:9 after canceling a call that is in the process of being connected from the client. This causes active H.323 calls to drop.
CSCve62662	A resource leak could lead to the H.323 Gateway component crashing. This leak was caused by a race condition between a media stream being setup and the call being torn down. In some situations, this prevents the resource being released when the call is torn down, and over time all resources are consumed.
CSCve49637	TX9000/IX5000 does not receive video after Hold/Resume if a Session Border Controller (SBC) is within the call path.
CSCve35856	If a logged in user calls into a space that they aren’t a member of using the WebRTC app, the log in box displays “Type passcode”, even if the passcode is optional.
CSCve18588	The H.323 Gateway could crash if a call was torn down while a new media stream for that call was being set up.

Cisco identifier	Summary
CSCve17230	In-call chat doesn't work in distributed calls between two Cisco Meeting App users when allocated to two different Call Bridges.
CSCve08092	When making an outgoing call to a Lync client with videoMode set to disabled, the call rings on the Lync client but then drops shortly afterwards.

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.
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.
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.
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 Home 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.
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
CSCve95813	A rare thread synchronization error can result in a media process crash. Users might experience a brief interruption in media while objects are moved to another media framework.
CSCve26277	Cisco Meeting Server doesn't respond to BFCPHello from HDX when BFCP mode is “server and client”.
CSCvf02105	Improvements have been made to 3 screen TIP endpoints dialling into a Meeting Server over a SIP trunk configured to use Early Offer. If you continue to see problems with the call dropping to a single screen call, then you are advised to set the SIP trunk from CUCM to the Cisco Meeting Server to use Delayed Offer.
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
CSCve26287	TIP endpoint doesn't display video when quality is below 720p.
CSCvk03337	Some TIP calls are failing with TIP negotiation timeout (this only affects 2.2.13 onwards).
CSCvj49594	Active Control does not work after hold/resume when a call traverses Cisco Unified Communications Manager and Cisco Expressway.

In addition there is the following limitation:

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

Cisco Legal Information

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

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

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

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

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

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

Cisco Trademark