Cisco Meeting Server

Cisco Meeting Server Release 3.6.2

Release Notes

12 January, 2023

Contents

What's changed

Version	Change
January 12, 2.2023	Updated Smart Licensing section
December 21, 2022	Maintenance release 3.6.2 See Resolved Issues.
December 01, 2022	Maintenance release 3.6.1 See Resolved Issues.
October 14, 2022	Updated Upgrade section
August 23, 2022	First release for version 3.6.

1 Introduction

This document describes the new features, improvements and changes in version 3.6 of the Cisco Meeting Server software.

The Cisco Meeting Server software can be hosted on:

- Cisco Meeting Server 2000, a UCS 5108 chassis with 8 B200 blades and the Meeting Server software pre-installed as the sole application.
- Cisco Meeting Server 1000, a Cisco UCS server pre-configured with VMware and the Cisco Meeting Server installed as a VM deployment.
- Or on a specification-based VM server.

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

Note: Cisco Meeting Management handles the product registration and interaction with your Smart Account for Smart Licensing support. Meeting Management 3.6 is required with Meeting Server 3.6.

- **Upgrade**: The recommended work flow is to first upgrade Meeting Management, complete Smart Licensing, and then upgrade Meeting Server.

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

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

1.1 Smart Licensing

From the 3.4 release onwards, Smart licensing is mandatory for Meeting Server. The support for traditional licensing has been deprecated from 3.4 and later releases. Customers are advised to move to Smart licensing.

For more information on Smart Licensing and upgrading Meeting Management, see Meeting Management Release Notes .

Note: Cisco Smart Licensing Cloud Certificates will be updated on January 15, 2023. Customers using Direct Mode for licensing between Meeting Management and Smart Licensing Portal should upgrade to version 3.6 to continue to use direct mode. If upgrade to version 3.6 is

---

not possible, customers can opt for SLR/PLR mode or on-premise satellite mode. The certificate update will not impact deployments that are using SLR/PLR or on-premise satellite with Meeting Management (3.5 or below).
If Meeting Management is not upgraded in time, Meeting Server will continue to work, but the license enforcement will be initiated. Meeting Management will be on a 90 day grace period, after which non-compliance notifications will be flashed on the participant's screen and audio prompts.

1.2 End of Software Maintenance

On release of Cisco Meeting Server software version 3.6, Cisco announced the time line for the end of software maintenance for the software in Table 1.

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

Cisco Meeting Server software version	End of Software Maintenance notice period
Cisco Meeting Server version 3.3.x	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes for Cisco Meeting Server version 3.3.x is August 22, 2022.
Cisco Meeting Server version 3.4.x	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes for Cisco Meeting Server version 3.4.x is December 17, 2022.

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

2 New features and changes in version 3.6

Version 3.6 of the Meeting Server software introduces the following new features and changes:

- Support for configurable options for video and content share
- Capturing packets in multiple pcap files on rotation
- Add logo in standard layouts
- Sharing files in a meeting
- Use a virtual or blurred background in a meeting

2.1 Support for configurable options for video and content share

Cisco Meeting Server provides configurable options to specify maximum resolutions for main video and shared content during calls. However, there are a few resolutions that the Meeting Server currently supports but the system administrators do not have the option to configure them. From version 3.6, these resolutions can be configured on Meeting Server, making all the supported resolutions for video and content share configurable. These resolutions are configurable only for video calls from SIP endpoints and does not apply for calls from web app.

The existing API parameters **`qualityMain`** and **`qualityPresentation`** under callLeg profile is modified to take new values in addition to the existing values.

2.1.1 API additions

The following API parameters are modified to take new values to set the resolutions for the video and content share respectively. It is supported on the following methods:

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

Parameter	Type/Value	Description
`qualityMain`	max1080p60	Restricts the maximum negotiated main video call quality for this callLeg based on limiting transcoding resources. max1080p60 - restricts the bridge to negotiating at most 1920x1080 screen size at 60 frames per second or equivalent transcoding resources.

Parameter	Type/Value	Description
qualityPresentation	max720p30	Restrict 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 callLegs which use a separate presentation stream. max720p30 - Restricts the Call Bridge to negotiating at most 1280x720 screen size at 30 frames per second or equivalent transcoding resources.

2.2 Capturing packets in multiple pcap files on rotation

In previous versions, the **pcap** MMP command captured the packets on the specified interface in a single file and stopped when you press Ctrl-C. From version 3.6, packets can be captured in multiple files, on rotation. When a pcap file size exceeds 500MB, the packets are captured in a new file. Meeting Server saves upto four pcap files with a total maximum file size limit of 2GB at any given time. Once the fourth pcap file size exceeds 500MB, the oldest pcap file is deleted and continues to capture packets in the new file. This feature allows the packets to be captured perpetually until the user stops.

Note: The packets will not be captured if the available memory on the device is less than 3GB.

For example, when the capture begins, the packets are captured in a file named **admin-a-20220620-100650.pcap**. Once the file size reaches 500MB, this file is renamed as **1-admin-a-20220620-100650.pcap**. As the pcap file sizes exceed 500MB the packets are captured in files **2-admin-a-20220620-100650.pcap** and **3-admin-a-20220620-100650.pcap**. The oldest file is **3-admin-a-20220620-100650.pcap** and the current packets are captured in **admin-a-20220620-100650.pcap**. The packets are captured in multiple files in rotation by deleting the oldest pcap file once the fourth file reaches the maximum file size of 500MB.

2.3 Add logo in standard layouts

Version 3.6 introduces the capability to add logos in a standard layout. Organizations can use this feature for branding purposes to display their logos on the participants' screen during the meeting.

This is a licensed feature and works if an active customization license is present in the Meeting Server. This feature is supported only on SIP endpoints.

Administrators can upload the logos that can be configured to display in certain positions, in a standard layout. To display the logo on the participant's screen, upload the logos to the Meeting Server using SFTP and configure them at the meeting level, using the **calls** and **callProfiles** API.

If the logo image is not uploaded or the customization license is not activated, the logo will not be rendered in the layout.

Note:

- Adding logos is supported only on standard layouts that includes fixed and dynamic layouts.
- This feature is not supported on web app.

In this feature:

- The logo images must be uploaded to the Meeting Server using SFTP.
- The logo image file can have a maximum resolution of 256*256 and in .png format for it to be rendered in the layout.
- For optimal usage of the screen space, the recommended image size is 128*128.
- If the deployment has a clustered environment, the logo file must be uploaded on all the Call Bridge nodes in the cluster.
- Logo can be placed in the following positions of the recipient's screen, in a standard layout:
  - Left top
  - Left bottom
  - Right top
  - Right bottom

2.3.1 API additions

New API parameters **`logoFileName`** and **`logoPosition`** are introduced to add the logo in the standard video layout. The parameters are supported on the following methods:

- POST to **`/callProfiles`**
- PUT to **`/callProfiles/<call profile id>/`**
- GET on **`/callProfiles/<call profile id>/`**
- POST to **`/calls`**
- PUT to **`/calls/<call id>/`**
- GET on **`/calls/<call id>/`**

Parameter	Type/Value	Description
`logoFileName`	String	Name of the image file that is uploaded using SFTP with file name restricted to 128 characters.

Parameter	Type/Value	Description
`logoPosition`	leftTop| leftBottom| rightTop| rightBottom	The position where the logo needs to be rendered on the recipient screen. If unset at all levels, the logo position defaults to `leftTop`.

2.4 Sharing files in a meeting

The file share feature was introduced as a beta feature in version 3.5. This feature enabled the web app participants to share files during a web app meeting. From version 3.6, file sharing will be a fully supported feature. File sharing uses MeetingApps services to enable participants to share files in the meeting.

2.4.1 Overview

File sharing allows web app participants with appropriate permissions to share files in a meeting. If file sharing is allowed for the meeting, a signed-in web app user can download the files. Only a signed-in user with appropriate permissions can share files in a meeting. With this feature:

- If file sharing is allowed for the meeting, only a signed-in web app user can download the files.
- Only a signed-in web app user with appropriate permissions can share files in a meeting.
- The shared file is available for download only during the meeting. Participants joining after a meeting has started can only view or download the files that are shared after they joined the meeting.
- File sharing supports a maximum of 5 files with a size limit of 10MB at a time.
- Participants can share all types of files except for the following file extensions:

  .exe, .bat, .bin, .com, .cmd, .inf, .ipa, .osx, .pif, .run, .wsh, .pkg, .dmg, .apk, .sh, .html, .asp, .js, .vbs, .wsf, .php, .scpt

---

Note:

- File share feature is not supported for web app participants joining as guest or participants joining through SIP endpoints, Lync, or Skype.
- Once a file is shared, it cannot be deleted by the participants in the meeting.

Refer to *Cisco Meeting Server web app Important Information* document for details on using File sharing feature in a meeting.

2.4.2 Deploying MeetingApps

A new service called MeetingApps has been implemented to support file sharing. The MeetingApps must be configured on a stand alone Meeting Server node without any other services. Depending on whether the participants are joining from an external or an internal network, MeetingApps can be configured on DMZ network or on internal network accordingly.

We recommend you configure MeetingApps on a stand alone Virtualized deployment of Meeting Server in a split-server deployment.

Note: MeetingApps services cannot be configured on Meeting Server 2000. It is recommended to configure the MeetingApps only on a spec based Virtualized deployment of Meeting Server. However, you can use Meeting server 2000 or Meeting Server 1000 as a Call Bridge or Web bridge along with Meeting Apps on VM deployments.

To enable file sharing in meetings where you have web app participants joining from internal and external network, the MeetingApps must be deployed on DMZ network. The MeetingApps must be assigned a publicly accessible IP address and the firewall ports must opened on DMZ for public access.

If file sharing is restricted only for participants joining a web app meeting internally, the MeetingApps can be deployed anywhere in the data center.

The MeetingApps can be configured on VM deployments of Meeting Server using the MMP command **`meetingapps`**.

File store capacity on MeetingApps is approximately 20 GB at a given point of time. Participants in the meeting will not be able to share the files if the file store capacity is exhausted within a period of 12 hours from the time the first file was shared. The file are deleted by an internal task that runs every 12 hours.

MeetingApps supports a maximum of 150 concurrent requests per second. This implies that a maximum of150 file upload or download requests can be processed by MeetingApps per second.

Web Bridges in your environment must be configured to talk to MeetingApps in order to upload or download the files shared in the meeting. The MeetingApps host name, port number and the secret key generated must be provided to configure the web bridge using the MMP command **`webbridge3 meetingapps add`**

For information on configuring MeetingApps refer to 3.6 Single Split Server Deployment Guide.

2.4.3 API and MMP additions

New API parameters and MMP commands are introduced to support file share. See Meeting Server 3.6 API Reference Guide and Meeting Server 3.6 MMP Command Line Reference Guide for more details.

2.5 Use a virtual or blurred background in a meeting

The background blur feature was introduced as a beta feature in version 3.4. This feature enabled Web app participants to blur their background in a meeting. From version 3.6, background blur is a fully supported feature. The feature has also been enhanced to provide better video quality even on low performance systems.

Blurring the background makes the surroundings appear out of focus hence hiding the details behind the participant and emphasizing the participant. Web app also introduces virtual backgrounds that enable participants to change their background with one of the preset backgrounds during a meeting. Participants can blur their background or apply virtual background only after they have joined the meeting and not on the preview page.

Refer to *Cisco Meeting Server web app Important Information document* for details on applying blur or virtual background in a meeting.

2.5.1 API Additions

A New API parameter **`backgroundBlurAllowed`** is introduced to enable or disable background blur at the call level.

For more information on APIs, see *Meeting Server 3.6 API Reference Guide*.

2.6 Summary of API additions and changes

API functionality for Meeting Server 3.6 includes the following new and modified API parameters.

New API parameter to add logo in the standard video layout

- **`logoFileName`** is introduced on
  - POST to **`/callProfiles`**
  - PUT to **`/callProfiles/<call profile id>/`**
  - GET on **`/callProfiles/<call profile id>/`**
  - POST to **`/calls`**
  - PUT to **`/calls/<call id>/`**
  - GET on **`/calls/<call id>/`**
- **`logoPosition`** is introduced on
  - POST to **`/callProfiles`**
  - PUT to **`/callProfiles/<call profile id>/`**
  - GET on **`/callProfiles/<call profile id>/`**

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

Modification to API objects and parameters

The **qualityMain** and **qualityPresentation** parameters, are modified to take new values to set the resolutions for the video and content share.

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

2.7 Summary of MMP additions

Version 3.6 supports the MMP changes described in this section.

Capturing packets in multiple pcap files on rotation

pcap command now captures packets in multiple files, on rotation. When a pcap file size exceeds 500MB, the packets are captured in a new file. Meeting server saves upto four pcap files with a total maximum file size limit of 2GB at any given time. Once the fourth pcap file size exceeds 500MB, the oldest pcap file is deleted and continues to capture packets in the new file.

3 Upgrading, downgrading and deploying Cisco Meeting Server software version 3.6.2

This section assumes that you are upgrading from Cisco Meeting Server software version 3.5. If you are upgrading from an earlier version, then you must first upgrade to 3.5 following the instructions in the 3.5 release notes, before following any instructions in this Cisco Meeting Server 3.6.2 Release Notes. This is particularly important if you have a Cisco Expressway connected to Meeting Server.

Note: Cisco has not tested upgrading from a software release earlier than 3.5.

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

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

3.1 Upgrading to Release 3.6.2

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

Note: If you have deployed a clustered database, before upgrading your Meeting Servers, uncluster all the nodes using the **`database cluster remove`** command. Users must uncluster the nodes, upgrade Meeting Server and cluster the nodes back using the MMP commands. See Cluster upgrade FAQ for detailed instructions.

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.

Note:
Meeting Server 3.0 introduced a mandatory requirement to have Cisco Meeting Management 3.0 (or later). Meeting Management handles the product registration and interaction with your Smart Account (if set up) for Smart Licensing support.

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

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

   `Cisco_Meeting_Server_3_6_2_CMS2000.zip`

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

   Hash (SHA-256) for upgrade.img file:
   00a195da6382587ef670397a912fc8a56f50107376b55f55449fdd5d7d63fe4d

   `Cisco_Meeting_Server_3_6_2_vm-upgrade.zip`

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

   Hash (SHA-256) for upgrade.img file:
   80a4bdc5c9f3396371fa0289d21613435ee7844be2604f7a5854c04f3c2b3c4b

   `Cisco_Meeting_Server_3_6_2.ova`

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

   For vSphere6, hash (SHA-512) for Cisco_Meeting_Server_3_6_2_vSphere-6_0:
   10d32eafe038c29689ab15348621c99dc65488c651e2598bf69caab49a61883f1eafe471e303e06bc324bac39a0c089aed6097966fb3273ed2438da4eac06c0e

   For vSphere6.5 and higher, hash (SHA-512) for Cisco_Meeting_Server_3_6_2_vSphere-6_5.ova:
   5d8129df5e61ed6c3f874869c656730747426c303113d0ce279560c904d28673437662a43d4605b8ffd97d7e96d4286d1fcf738bfce5272d7a9e96c4e2614028

2. To validate the OVA file, the checksum for the 3.6.2 release is shown in a pop up box that appears when you hover over the description for the download. In addition, you can check the integrity of the download using the SHA-512 hash value listed above.
3. Using an SFTP client, log into the MMP using its IP address. The login credentials will be the ones set for the MMP admin account. If you are using Windows, we recommend using the WinSCP tool.

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

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

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

      `upgrade list`
   c. Check that this checksum matches the checksum shown above.
6. To apply the upgrade, use the SSH connection to the MMP from the previous step and initiate the upgrade by executing the **`upgrade`** command.
   a. Initiate the upgrade by executing the upgrade command.
      `upgrade <image_name>.img. For example: upgrade upgrade_spa.img`
   b. The Server/ virtualized server restarts automatically: allow 10 minutes for the process to complete.
7. Verify that Meeting Server is running the upgraded image by re-establishing the SSH connection to the MMP and typing:
   `version`
8. Update the customization archive file when available.
9. You have completed the upgrade.

3.2 Downgrading

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

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

   The Server/ virtualized server will restart automatically – allow 10-12 minutes for the process to complete and for the Web Admin to be available after downgrading the server.
3. Log in to the Web Admin and go to **Status > General** and verify the new version is showing under **System status**.

4. Use the MMP command **`factory_reset app`** on the server and wait for it to reboot from the factory reset.
5. Restore the configuration backup for the older version, using the MMP command **`backup rollback <name>`** command.

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

   The Meeting Server will reboot to apply the backup file.

   For a clustered deployment, repeat steps 1-5 for each node in the cluster.

6. a. In the case of XMPP clustering, if applicable, you need to re-cluster XMPP:
   a. Pick one node as the XMPP primary, initialize XMPP on this node
   b. Once the XMPP primary has been enabled, joining any other XMPP nodes to it.
   c. Providing you restore using the backup file that was created from the same server, the XMPP license files and certificates will match and continue to function.
7. Finally, check that:
   - the Web Admin interface on each Call Bridge can display the list of coSpaces.
   - dial plans are intact,
   - XMPP service is connected, if applicable,
   - no fault conditions are reported on the Web Admin and log files.
   - you can connect using SIP and Cisco Meeting Apps (as well as Web Bridge if that is supported).

   The downgrade of your Meeting Server deployment is now complete.

3.3 Cisco Meeting Server Deployments

To simplify explaining how to deploy the Meeting Server, deployments are described in terms of three models:

- single combined Meeting Server – all Meeting Server components (Call Bridge, Web Bridge 3, Database, Recorder, Uploader, Streamer and TURN server) are available, the Call Bridge and Database are automatically enabled but the other components can be individually enabled depending upon the requirements of the deployment. All enabled components reside on a single host server.

- single split Meeting Server – in this model the TURN server, Web Bridge 3, and MeetingApps are enabled on a Meeting Server located at the network edge in the DMZ, while the other components are enabled on another Meeting Server located in the internal (core) network.
- the third model covers deploying multiple Meeting Servers clustered together to provide greater scale and resilience in the deployment.

Deployment guides covering all three models are available here. Each deployment guide is accompanied by a separate Certificate Guidelines document.

Points to note:

The Cisco Meeting Server 2000 only has the Call Bridge, Web Bridge 3, and database components. It is suited for deployment on an internal network, either as a single server or a cascade of multiple servers. The Cisco Meeting Server 2000 should not be deployed in a DMZ network. Instead if a deployment requires firewall traversal support for external Cisco Meeting Server web app users, then you will need to also deploy either:

- a Cisco Expressway-C in the internal network and an Expressway-E in the DMZ, or
- a separate Cisco Meeting Server 1000 or specification-based VM server deployed in the DMZ with the TURN server enabled.

The Cisco Meeting Server 1000 and specification-based VM servers have lower call capacities than the Cisco Meeting Server 2000, but all components (Call Bridge, Web Bridge 3, Database, Recorder, Uploader, Streamer and TURN server) are available on each host server. The Web Bridge 3, Recorder, Uploader, Streamer and TURN server require enabling before they are operational.

4 Bug search tool, resolved and open issues

You can now use the Cisco Bug Search Tool to find information on open and resolved issues for the Cisco Meeting Server, including descriptions of the problems and available workarounds. The identifiers listed in these release notes will take you directly to a description of each issue.

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

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

1. Enter the bug identifier in the **Search** field and click **Search**.

To look for information when you do not know the identifier:

1. Type the product name in the **Search** field and click **Search**

   or,

   in the **Product** field select **Series/Model** and start typing `Cisco Meeting Server`, then in the **Releases** field select **Fixed in these Releases** and type the releases to search for example `3.2`.
2. From the list of bugs that appears, filter the list using the *Modified Date*, *Status*, *Severity*, *Rating* drop down lists.

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

4.1 Resolved issues

Note: Refer to the Cisco Meeting Server web app Important information guide for information on resolved issues affecting web app.

Issues seen in previous versions that are fixed in 3.6.2

Cisco identifier	Summary
CSCwd11917	When two endpoints using dual cameras (Panorama) are in a distributed call over a clustered deployment, the video quality drops with low frame and bit rates after a third endpoint joins the meeting over the distributed link. This drop was due to faulty internal messaging, and it is fixed in the 3.6.2 release. To maintain the video quality, the administrators must disable the **`passthroughMode`** option in the **`compatabilityProfile`** API. It is also recommended to set both, the SIPs and peer link bandwidth to 4 Mbps.

Issues seen in previous versions that are fixed in 3.6.1

Cisco identifier	Summary
CSCwa01752	The syslogs generated using Meeting Server 2000 does not include some of the information required for web app user identification.
CSCwd16194	In rare cases, the Scheduler on Meeting Server 2000 fails to send email notifications, when using SMTP with Authenticated login configuration.
CSCwc01047	Unauthenticated HTTPS request can trigger segmentation fault and edge server crash.
CSCwb60392	When a participant is sharing content and is moved to lobby, the participant's screen is still visible to other participants in the meeting.

Issues seen in previous versions that are fixed in 3.6.

Cisco identifier	Summary
CSCwa40239	When the Email invites are sent using the Scheduler, all the email address in the participant list must be valid. Scheduler might not send emails to any of the participants from the list, even if one of the email address is invalid.
CSCwc68615	To avoid the .bak file from getting corrupted, copying the intermediate backup snapshot file (.bak) over SFTP should be denied until the backup snapshot process is completed.
CSCvy61122	Occasionally, an error message " System is currently unavailable" is displayed when the users attempt to join a web app meeting.
CSCvz28836	The peer links that get disconnected during network interruptions are not restored even after the network is reconnected.
CSCwc17966	Meeting Server crashes if the co-space URI has 14 or more characters in length and ends with a special character.
CSCwa68125	When a participant applies a custom layout, the video in the fixed pane is not displayed through the entire screen.

4.2 Open issues

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

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

Cisco identifier	Summary
CSCwb77929	In a deployment with multiple Web Bridge, web app participants can see the Meeting notes only if they are connected to the same webbridge where the notes was saved and published initially.

Cisco identifier	Summary
CSCwa83782	A conference is booked on TMS as Automatic connect type and one of the participants is joining the conference through an unmanaged device. When the conference starts, the participant is called by CMS/TMS, but Meeting Serverdisconnects the call after some time.
CSCvz01886	When a participant's role does not have permissions to share video and presentation, then the role is changed and they have permissions to share video and presentation, the presentation is not visible to other participants when they share content.
CSCvw61547	On very rare occasions, calls through a Meeting Server TURN component may fail to connect or may lack a media channel. An error similar to " TURN 437 allocation mismatch in state RefreshTurnAllocationPending" will be seen in the Call Bridge syslog.
CSCvt74033	When content is being shared and an event happens to trigger a Webex Room Panorama to drop from sending two video streams to one, the video frame rate being received by a remote endpoint from the Room Panorama can drop noticeably.
CSCvh23039	The Uploader component does not work on tenanted recordings held on the NFS.

4.2.1 Known limitations

- From version 3.1, Cisco Meeting Server supports TURN short-term credentials. This mode of operation can only be used if the TURN server also supports short-term credentials, such as the Meeting Server TURN server in version 3.1 onwards. Using Cisco Meeting Server with Expressway does not support short-term credentials.

5 Meeting Server platform maintenance

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

5.1 Cisco Meeting Server 1000 and other virtualized platforms

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

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

5.2 Cisco Meeting Server 2000

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

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

5.3 Call capacities

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

Table 2: Call capacities across Meeting Server platforms

Type of calls	Cisco Meeting Server 1000 M4	Cisco Meeting Server 1000 M5	Cisco Meeting Server 1000 M5v2	Cisco Meeting Server 2000	Cisco Meeting Server 2000 M5v2
Full HD calls 1080p60 video 720p30 content	24	24	30	175	218
Full HD calls 1080p30 video 1080p30/4K7 content	24	24	30	175	218

Type of calls	Cisco Meeting Server 1000 M4	Cisco Meeting Server 1000 M5	Cisco Meeting Server 1000 M5v2	Cisco Meeting Server 2000	Cisco Meeting Server 2000 M5v2
Full HD calls 1080p30 video 720p30 content	48	48	60	350	437
HD calls 720p30 video 720p5 content	96	96	120	700	875
SD calls 480p30 video 720p5 content	192	192	240	1000	1250
Audio calls (G.711)	1700	2200	2200	3000	3000

Table 3 provides the call capacities for a single or cluster of Meeting Servers compared to load balancing calls within a Call Bridge Group.

Table 3: Meeting Server call capacity for clusters and Call Bridge groups

Cisco Meeting Server platform		Cisco Meeting Server 1000 M4	Cisco Meeting Server 1000 M5	Cisco Meeting Server 1000 M5v2	Cisco Meeting Server 2000	Cisco Meeting Server 2000 M5v2
Individual Meeting Servers or Meeting Servers in a cluster (notes 1, 2, 3, and 4) and Meeting Servers in a Call Bridge Group	1080p30 720p30 SD Audio calls	48 96 192 1700	48 96 192 2200	60 120 240 2200	350 700 1000 3000	437 875 1250 3000
	HD participants per conference per server	96	96	120	450	450
	web app call capacities (internal calling & external calling on CMS web edge): Full HD HD SD Audio calls	48 96 192 500	48 96 192 500	60 120 240 500	350 700 1000 1000	437 875 1250 1250
Meeting Servers in a Call Bridge Group	Call type supported	Inbound SIP Outbound SIP				
	Load limit	96,000	96,000	120,000	700,000	875,000

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

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

Note 3: Up to 21,000 HD concurrent calls per cluster (24 nodes x 875 HD calls) applies to SIP or web app calls.

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

Note 5: Table 3 assumes call rates up to 2.5 Mbps-720p5 content for video calls and G.711 for audio calls. Other codecs and higher content resolution/framerate will reduce capacity. When meetings span multiple call bridges, distribution links are automatically created and also count against a server's call count and capacity. Load limit numbers are for H.264 only.

Note 6: The call setup rate supported for the cluster is up to 40 calls per second for SIP calls and 20 calls per second for Cisco Meeting Server web app calls.

5.4 Cisco Meeting Server web app call capacities

This section details call capacities for deployments using Web Bridge 3 and web app for external and mixed calling. (For internal calling capacities, see Table 3.)

5.5 Cisco Meeting Server web app call capacities – external calling

Expressway (Large OVA or CE1200) is the recommended solution for deployments with medium web app scale requirements (i.e. 800 calls or less). Expressway (Medium OVA) is the recommended solution for deployments with small web app scale requirements (i.e. 200 calls or less). However, for deployments that need larger web app scale, from version 3.1 we recommend Cisco Meeting Server web edge as the required solution.

For more information on using Cisco Meeting Server web edge solution, see Cisco Meeting Server 3.1 Release notes.

External calling is when clients use Cisco Meeting Server web edge, or Cisco Expressway as a reverse proxy and TURN server to reach the Web Bridge 3 and Call Bridge.

When using Expressway to proxy web app calls, the Expressway will impose maximum calls restrictions to your calls as shown in Table 4.

Note: If you are deploying Web Bridge 3 and web app you must use Expressway version X12.6 or later, earlier Expressway versions are not supported by Web Bridge 3.

Table 4: Cisco Meeting Server web app call capacities – using Expressway for external calling

Setup	Call Type	CE1200 Platform	Large OVA Expressway	Medium OVA Expressway
Per Cisco Expressway (X12.6 or later)	Full HD	150	150	50
	Other	200	200	50

The Expressway capacity can be increased by clustering the Expressway pairs. Expressway pairs clustering is possible up to 6 nodes (where 4 are used for scaling and 2 for redundancy), resulting in a total call capacity of four times the single pair capacity.

Note: The call setup rate for the Expressway cluster should not exceed 6 calls per second for Cisco Meeting Server web app calls.

5.6 Cisco Meeting Server web app capacities – mixed (internal + external) calling

Both standalone and clustered deployments can support combined internal and external call usage. When supporting a mix of internal and external participants the total web app capacity will follow Table 3 for Internal Calls and if using Cisco Meeting Server web edge solution for external calling. However, if using Expressway at the edge, the number of participants within the total that can connect from external is still bound by the limits in Table 4.

For example, a single standalone Meeting Server 2000 with a single Large OVA Expressway pair supports a mix of 1000 audio-only web app calls but the number of participants that are external is limited to a maximum of 200 of the 1000 total.

6 Related user documentation

The following sites contain documents covering installation, planning and deployment, initial configuration, operation of the product, and more:

- Release notes (latest and previous releases): https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-release-notes-list.html
- Install guides (including VM installation, Meeting Server 2000, and using Installation Assistant): https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-guides-list.html
- Configuration guides (including deployment planning and deployment, certificate guidelines, simplified setup, load balancing white papers, and quick reference guides for admins): https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-and-configuration-guides-list.html
- Programming guides (including API, CDR, Events, and MMP reference guides and customization guidelines): https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-programming-reference-guides-list.html
- Open source licensing information: https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-licensing-information-listing.html
- Cisco Meeting Server FAQs: https://meeting-infohub.cisco.com/faq/category/25/cisco-meeting-server.html
- Cisco Meeting Server interoperability database: https://tp-tools-web01.cisco.com/interop/d459/s1790

7 Accessibility Notice

Cisco is committed to designing and delivering accessible products and technologies.

The Voluntary Product Accessibility Template (VPAT) for Cisco Meeting Server is available here:

http://www.cisco.com/web/about/responsibility/accessibility/legal_regulatory/vpats.html#telepresence

You can find more information about accessibility here:

www.cisco.com/web/about/responsibility/accessibility/index.html

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