Cisco Meeting Server and web app

Release 3.7.2

Release Notes

08 August, 2023

Contents

What's changed

Version	Change
August 8, 2023	Maintenance release 3.7.2 See Resolved Issues
June 13, 2023	Maintenance release 3.7.1 See Resolved Issues
March 16, 2023	First release for version 3.7

1   Introduction

This document describes the new features, improvements and changes in version 3.7 of the Cisco Meeting Server software and Cisco Meeting Server web app.

1.1   Cisco Meeting Server

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 3.7 is required with Meeting Server 3.7.

- **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: Microsoft RTVideo and consequently Lync 2010 on Windows and Lync 2011 on Mac OS, will not be supported going forward. However, support for Skype for Business and Office 365 will continue.

1.2   Cisco Meeting Server web app

Cisco Meeting Server web app (web app) is a browser-based client for Cisco Meeting Server that lets users join meetings (audio and video) and share what is on their screen.

Cisco Meeting App for WebRTC is removed in Cisco Meeting Server version 3.0 and later. You need to use Cisco Meeting Server web app instead of Cisco Meeting App for WebRTC.

Note: Cisco Meeting App for desktop, iOS and WebRTC are no longer supported in Cisco Meeting Server since version 3.0.

1.3 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 .

1.4 End of Software Maintenance

On release of Cisco Meeting Server software version 3.7, 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 3.5.x	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes for Cisco Meeting Server version 3.5.x is July 15, 2023.

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

2 Cisco Meeting Server

This section of the document lists the new features and changes implemented in Meeting Server version 3.7.

2.1 Enhancements in 3.7.2

- Configuring screen resolution for content shared in web app

2.2 What's new in Cisco Meeting Server 3.7

Following are the new features and changes introduced in this release:

- Adding logo in custom and standard screen layouts
- Improvements in syslogs generated on 2000
- Configuring default join method for web app users
- Adding custom background images for virtual background
- Updating status of Jabber users while in a web app meeting
- Improved video quality in conferences with dual camera endpoints
- Configuring auto prioritization of audio over content share and video during web app meeting
- Serviceability Enhancements

2.2.1 Configuring screen resolution for content shared in web app

 In version 3.7.1, the maximum resolution for screen sharing was restricted to 720p and was not configurable. Version 3.7.2 introduces the option to set the maximum resolution of the presenter's screen, while sharing content in web app meeting. However, in varying network conditions, the screen resolution adapts based on available bandwidth but will not exceed the maximum limit specified. For example, if the limit is set to 720p, the screen share resolution can go lower but not exceed 720p.

Screen resolution can be set as 720p, 1080p or unrestricted. By selecting unrestricted web app relies on browser to set the resolution for content share.

This feature is implemented using the new `contentResolution` parameter in the `webBridgeProfiles` API.

2.2.1.1 API additions

A new API parameter `contentResolution` is added to the `webbridgeProfile` API. This parameter is supported on POST, PUT and GET methods on `/webBridgeProfiles/`.

Request parameters	Type/ Value	Description/ Notes
`contentResolution`	720p|1080p|unrestricted	The maximum resolution of the presenter's screen while sharing content in web app.

2.2.2 Adding logo in custom and standard screen layouts

From version 3.7, logos can be configured in custom and standard layouts and is supported on both web app and SIP endpoints. Organizations can use this feature to display their logos on the participants' screens during the meeting, thereby using them for branding purposes. This is a licensed feature and works if an active customization license is present in the Meeting Server.

Administrators can upload logos that can be configured to display in certain positions in standard and custom layouts. 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.

In this feature:

- The logo images must be uploaded using SFTP, to the server that hosts Call Bridge(for SIP) and Web Bridge(for web app).

- The logo image file must be in .png format with a maximum resolution of 256*256 pixels and a file size of less than 64 kb. The logo image will not be rendered if the image size or the resolution is more than the specified limit and is recorded as an error in the syslog entries.

- For optimal usage of the screen space, the recommended image resolution is 128*128.

- Due to a change in the image file directory in 3.7, logo images uploaded in the previous version (3.6) will not be rendered after upgrading to Meeting Server 3.7. Therefore, it is recommended to delete the old files and upload new files, with same name or different name. This is needed to ensure new files copied to SFTP server go into right file directory in 3.7 release.

- If the deployment has a clustered environment, upload the logo files on all the Call Bridge nodes in the cluster.

- Logo can be placed in the following positions on the recipient's screen:
  - Left top
  - Left bottom
  - Right top
  - Right bottom

Choose the Left top or Left bottom positions to prevent the logo from covering the participant count or the recording icon on the right-hand side of the web app or SIP screens.

Note: While sharing content, the logo position on web app will remain as configured on Meeting Server. However the logo on SIP endpoints, will be displayed in the video pane.

2.2.2.1 API additions

The existing API parameters `logoFileName` and `logoPosition` can be used to add logo in a custom 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.
`logoPosition`	leftTop| leftBottom| rightTop| rightBottom	The position where the logo has to be rendered on the recipient screen. If unset at all levels, the logo position defaults to `leftTop`.

2.2.3 Improvements in syslogs generated on Meeting Server 2000

Version 3.7 introduces improvements to the syslogs generated on Meeting Server 2000. In previous releases, administrators were unable to map the participant's IP address with the Participant ID. Improvements have been made in the syslog to show **Join call: <participant id> IP address** that enables the administrators to identify the participants joining through web app with the corresponding IP address. The participant ID can be further mapped with IP address, alias and guest ID.

The syslog entries from Meeting Server 2000 will now include participant ID as shown below:

2022-10-13T09:03:36.196Z .info cms75.xchange.lab cms wb3_frontend: [`Join call:b6d3e7de-8f1b-4b04-9ac5-07f7e5863726`] 10.65.79.171 - - [13/Oct/2022:09:03:36 +0000] status 200 " POST /api/join HTTP/1.1" bytes_sent 902 http_referer " https://10.209.81.75:4443/" http_user_agent " Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36" to upstream 192.0.2.2:9000: upstream_response_time 0.024 request_time 0.024 msec 1665651816.195 upstream_response_length 926 200

2.2.4 Configuring default method to join a web app meeting

Version 3.7 introduces the new `lobbyProfiles` API to configure the default method to join a web app meeting to, **audio and video** or **presentation only** modes. This parameter is configured for each participant joining as a guest user or as a signed in member of a space. Administrators can configure and apply this profile at different levels to suit their requirements. The web app joining page will accordingly, default to **audio and video** or **presentation only** mode. However, the participants can override the configured default method, by selecting the options listed under **More Ways to Join** in the **Web app joining options** screen.

Note: The default join method can be configured for web app participants only. Dial-in options are not configurable.

2.2.4.1 API additions

A new API profile `lobbyProfiles` is introduced to configure the default joining method. This profile includes parameters that control the options available for a web app user at the joining screen. It can optionally associate itself with coSpace, coSpaceTemplates, coSpaceUser, accessMethod, accessMethodTemplates, tenant objects, and system profiles.

Setting up and modifying lobbyProfiles

- Creating: POST to **/lobbyProfiles** node
- Modifying: PUT to **/lobbyProfiles/<lobby Profile id>**

Retrieving lobbyProfiles

- GET method on **/lobbyProfiles/<lobby Profile id>**

Parameter	Type/Value	Description
`name` **(optional)**	String	Optional name label to help identify this profile (maximum size 200 bytes)
`joinMethod` **(optional)**	unset | presentationOnly | **audioVideo**	One of **presentationOnly** or **audioVideo**. This determines if a webapp participant will join with presentation only or as an audio video participant.
		The usual rules for the hierarchy of lobbyProfiles apply to this parameter. If unset at all levels of the hierarchy, it defaults to the existing method of **audioVideo**.
		For guest users, the parameter follows the hierarchy: **accessMethod > coSpaces > tenant > system/profiles**.
		For users who are trying to join a space that they are a member of, using the **Join** button, the parameter follows the hierarchy: **coSpaceUsers > accessMethod > coSpaces > tenant > system/profiles**.

`lobbyProfile` is supported on the following nodes for POST, PUT and GET methods:

- `/coSpaces/<cospace id>`

- `/coSpaces/<cospace id>/accessMethods/<access method id>`

- `/coSpaces/<cospace id>/coSpaceUsers/<cospace user id>`

- `/system/profiles`

- `/tenants/<tenant id>`

- `/coSpaceTemplates/<template id>`

- `/coSpaceTemplates/<coSpace template id>/<accessMethodsTemplates>/<access method template id>`

Parameter	Type/Value	Description
`lobbyProfile`	ID	If provided, associates the lobbyProfile with the specified node.

2.2.5 Adding custom background images for virtual background

Version 3.6 included a predefined set of background images that web app participants could use as their background. Version 3.7 gives administrators the ability to upload background images to the Meeting Server, which will be rendered in web app, for the participants to use as their background.

The branding files for web app are placed in an archive file such as a zip file. Administrators can upload the background images to this folder. In addition, a `utils.json` file containing the count of images to be displayed as thumbnails in the web app must be created and placed in this folder.

The background images and `utils.json` file, along with the existing web branding files, if any, must be placed together and compressed into a zip file. The zip file can either be uploaded to the Meeting Server (Web Bridge) via SFTP (locally) or host the file remotely on any file-share server (remote branding). If the file is hosted locally, the zip file must be named **web_ branding**.zip.

The uploaded images will replace the existing predefined images in the web app library and the participants will have only the uploaded images to choose from. If the images are not uploaded in the Meeting Server or the image count in the json file is set to 0, web app displays the existing images from the library.

To upload the background images:

- The image must have a 16:9 aspect ratio.

- Images must have a minimum resolution of 1280x720 pixels.

- For optimal image quality, the recommended image resolution is 1920x1080 pixels.

- Each image can have a maximum file size of 1.5 MB. However, the branding file containing all the background images and other branding images, can have a maximum file size of 15 MB before compressed into a zip file.

- A json file, utils.json, must be created to specify the number of images to be displayed in web app. The count of the images to be displayed in web app must be specified in the following format:
  {
  " vb_count" : <count>
  }
  " vb_count" indicates the number of images to be listed as thumbnails in web app.
  For example,
  {
  " vb_count" :12
  }

- The count in the json file must be less than or equal to the number of images added to the zip file. If the count specified is more than the actual number of images uploaded in the zip file, additional thumbnails will be displayed without any image.

- The image files must be in .jpeg format with the file naming convention of `vb_images_<image number>.jpeg`. The image number must be in the sequence 1, 2, 3, 4, etc, for example, vb_images_1.jpeg, vb_images_2.jpeg, and so on. Any missing image number will be rendered as a blank thumbnail in web app.

- The zip file created using Mac device may sometimes contain extra files in it. It is recommended to check the zipped file before hosting.

Note: The background images will be picked up after the web bridge/ call bridge is restarted, that will affect any ongoing meetings. Therefore, it is recommended to not upload the images, while a Cisco Meeting Server web app meeting is in progress.

2.2.6 Updating status of Jabber users while in a web app meeting (Beta support)

Cisco Jabber users, in an enterprise, can join meetings hosted on Cisco Meeting Server via web app. From version 3.7, Meeting Server can be configured to update the presence status of Jabber users, while they are in a Cisco Meeting Server web app meeting. This feature is implemented by configuring Meeting Server with a Cisco Unified Communications Manager node.

For presence to be updated on Jabber:

- Meeting Server login ID should be email and it should map to $mail$ attribute of AD.

- In Cisco Unified Communications Manager, the same user should have $mail$ attribute mapped to Directory URI field.

- Jabber login can happen either through Directory URI or User ID field from Cisco Unified Communications Manager.

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

In this feature:

- When a Jabber user signs into web app and joins a meeting, Meeting Server updates the Jabber status to 'In a meeting, In a call' and reverts to their previous status after the user ends the meeting.

- Meeting Server does not update the jabber status in the following cases:

  - If the Jabber user is in another meeting/call while joining the web app meeting Meeting Server does not update the Jabber status.

  - If the Jabber user has set their status to **DND – Do not disturb** before joining the web app meeting, Meeting Server does not update the Jabber status.

  - If the user updates the Jabber status manually anytime during the web app meeting, Meeting Server does not override the manually updated user status.

Note:
- This feature does not support web app participants joining as guest or participants joining through SIP endpoints, Lync, or Skype.

- While this feature supports https, Meeting Server will not validate the certificates.

- Meeting Server will not update the presence for content share.

To update the user presence, configure the Meeting Server with a Cisco Unified Communications Manager node that provides AXL service. It supports only a single cluster of IMP servers, i.e., 3 Presence Redundancy Groups of 6 IMPS Nodes. Only one Cisco Unified Communications Manager can be configured on the Meeting Server. The Meeting Server updates the IMP server with the presence status of the users. Jabber then fetches these details from the IMP server and updates the user presence accordingly.

Administrators must provide the hostname/IP address of the Cisco Unified Communications Manager and the Application user credentials of AXL and IMP servers, using the new MMP command `callbridge ucm add <hostname/IP> <axl_user> <presence_user>`. The following users must be created on the Cisco Unified Communications Manager node:

- AXL user – <axl_user> – This user is an application user. Administrators must create a group with the role `Standard AXL API Access`, and assign it to the user.

- Presence user - <presence_user> - This user is an application user with groups **Admin-3rd Party Api** and **Third party Application Users**.

After adding the Cisco Unified Communications Manager to the Meeting Server, the administrators can validate the status of the AXL service and IMP service using the MMP commands `callbridge imps <hostname/IP> <presence_user> presence_ service status` and `callbridge ucm <hostname/IP> axl_service status` respectively.

2.2.6.1 MMP additions

The following MMP commands are introduced for updating the user status on jabber.

Command / Examples	Description
`callbridge ucm add <host-name/IP> <axl_user> <pres-ence_user>`	Adds a CUCM node to the Meeting Server. The command prompts the user to enter the password for the AXL user and presence user.
`callbridge ucm del <host-name/IP>`	Deletes the CUCM from the server.
`callbridge ucm <hostname/IP> axl_service status`	Validates the status of the AXL service. The command prompts the user to enter the password for the AXL user.
`callbridge imps <hostname/IP> <presence_user> presence_ser-vice status`	Validates the status of the presence service. The command prompts the user to enter the password for the presence user.
`callbridge ucm list`	Lists the details of the CUCM added to the Meeting Server along with its hostname/IP, AXL user and presence user.

2.2.7 Improved video quality in conferences with dual camera endpoints

Version 3.7 introduces enhancements in the Meeting Server to improve the video quality of conferences that have more than two camera endpoints (panorama). Additionally, a new `passthroughDualCamera` API parameter has been introduced on the `compatibilityProfiles` API that transcodes the video on the panorama endpoints.

This parameter must be disabled, only if the `passthroughMode` parameter of the existing API setting is enabled. Depending on the requirements, administrators can disable either the `passthroughMode` or `passthroughDualCamera` parameter.

Note: It is recommended to set the minimum bit rate of SIP RX/TX and peer link to 4 Mbps before placing the calls in conferences with dual camera end points.

2.2.7.1 API Additions

A new API parameter `passthroughDualCamera` is introduced to improve the video quality in conferences with more than two dual camera endpoints. The parameter is supported on the following methods:

- POST to **/compatibilityProfiles**

- PUT to **/compatibilityProfiles/<compatibility profile id>**

Parameter	Type/Value	Description
passthroughDualCamera	**enabled**|disabled	• enabled — Does not transcode video for dual camera endpoint and peer link. • disabled — Transcodes video for dual camera endpoint and peer link. Note: Disable this parameter only if **passthroughMode** is enabled. This parameter is void if **passthroughMode** is disabled.

2.2.8 Configuring auto prioritization of audio over content share and video during web app meeting

Version 3.7 introduces support for auto prioritization of audio over content share and video in a web app meeting. In low bandwidth scenarios, web app takes automatic actions to turn off the video and content share retaining the audio. As the network improves, web app restores the video and content share ensuring the best user experience in all scenarios of an unstable network.

Administrators can configure this feature using the new MMP command introduced on the Meeting Server. If this feature is enabled, web app turns off/ on the video and content share in low and unstable network scenarios. Administrators can disable this feature if they do not want web app to take automatic actions.

2.2.8.1 MMP Additions

Command/Examples	Description/Notes
webbridge3 audiopriflag (enable|disable)	Enables or disables the auto prioritization feature in web app. If the command is not configured, this feature is enabled by default. Enable - If enabled, web app turns off the video and content share in low bandwidth scenarios. Disable - If disabled, web app does not take any action in an unstable network.

2.2.9 Serviceability Enhancements

When upgrading a clustered database deployment, all nodes in the deployment must be unclustered. From version 3.7, Meeting Server will display a message to notify the users about this requirement.

Meeting Server identifies if the database cluster is enabled in the server configuration and accordingly notifies the user to uncluster the nodes before upgrading. Users can choose to abort the upgrade process by pressing **CTRL+C** within 20 seconds.

2.3 Summary of API additions and changes

API functionality for Meeting Server 3.7 includes the following new API profiles and parameters.

New API profile is introduced with the following parameters to configure the default method to join a web app meeting:

- **lobbyProfile** with API parameters `name` and `joinMethod` is introduced on:
  - POST to **/lobbyProfiles** node
  - PUT to **/lobbyProfiles/<lobby Profile id>**
  - GET method on **/lobbyProfiles/<lobby Profile id>**

- `lobbyProfile` is supported on the following nodes for POST, PUT and GET methods:
  - `/coSpaces/<cospace id>`
  - `/coSpaces/<cospace id>/accessMethods/<access method id>`
  - `/coSpaces/<cospace id>/coSpaceUsers/<cospace user id>`
  - `/system/profiles`
  - `/tenants/<tenant id>`
  - `/coSpaceTemplates/<template id>`
  - `/coSpaceTemplates/<coSpace template id>/<accessMethodsTemplates>/<access method template id>`

New API parameter to improve the video quality in conferences with more than two dual camera endpoints

- `passthroughDualCamera` is introduced on:
  - POST to `/compatibilityProfiles`
  - PUT to `/compatibilityProfiles/<compatibility profile id>`

API parameter enhanced to support adding logo in the custom 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>/**

2.4 Summary of MMP additions and changes

Version 3.7 supports the MMP additions described in this section.

Updating status of jabber users while in a web app meeting

The Meeting Server and CUCM node configuration details are provided using the new MMP commands listed below:

Command / Examples	Description
`callbridge ucm add <host-name/IP> <axl_user> <pres-ence_user>`	Adds a CUCM node to the Meeting Server. The command prompts the user to enter the password for the AXL user and presence user.
`callbridge ucm del <host-name/IP>`	Deletes the CUCM from the server.
`callbridge ucm <hostname/IP> axl_service status`	Validates the status of the AXL service. The command prompts the user to enter the password for the AXL user.
`callbridge imps <hostname/IP> <presence_user> presence_ser-vice status`	Validates the status of the presence service. The command prompts the user to enter the password for the presence user.
`callbridge ucm list`	Lists the details of the CUCM added to the Meeting Server along with its hostname/IP, AXL user and presence user.

Enabling auto prioritization of audio and content share over video during web app meeting

Administrators can enable/ disable the auto prioritization of audio and content share over video:

Command/Examples	Description/Notes
webbridge3 audiopriflag (enable|disable)	Enables or disables the auto prioritization feature in web app. If the command is not configured, this feature is enabled by default. Enable – If enabled, web app turns off the video and content share in low bandwidth scenarios. Disable – If disabled, web app does not take any action in an unstable network.

2.5 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

3 Upgrading, downgrading and deploying Cisco Meeting Server software version 3.7.2

This section assumes that you are upgrading from Cisco Meeting Server software version 3.6. If you are upgrading from an earlier version, then you must first upgrade to 3.6 following the instructions in the 3.6 release notes, before following any instructions in this Cisco Meeting Server 3.7.2 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 3.6.

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 3.7.2

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 complete 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_7_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:
   41a05978f8bbbd23bc4e5dfe5ed2e58228c19a483288e167c548b28cd9a35634

   `Cisco_Meeting_Server_3_7_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:
   fb5b73ff249b7be70977b280b0cddb5ab749b596a046251015775b0fbd73ed10

   `Cisco_Meeting_Server_3_7_2.ova`

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

   For vSphere6.5 and higher, hash (SHA-512) for Cisco_Meeting_Server_3_7_2_vSphere-6_5.ova:
   9a7909256dab47102d005b7cc39452cdc6f64645ab8a478d7fc011bfe33deff1bebe41ca9f4212a05d102fda1d606f83adabea78a2893cbfb8a3aad6f815fc31d3

2. To validate the OVA file, the checksum for the 3.7.2 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.

   Note: From version 3.7, Meeting server does not support ESXi versions 6.0 and below. The .ova files for these versions (ESXi 6.0/5.5) will not be provided.

   ---

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. Finally, check that:

- the Web Admin interface on each Call Bridge can display the list of coSpaces.

- dial plans are intact,

- 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 Cisco Meeting Server web app

This section of the document describes the new features, changes in this release of the Cisco Meeting Server web app.

4.1 What's new in Cisco Meeting Server web app

Enhancements in 3.7.1

- [Default resolution for web app presentation](#)

Web app version 3.7 introduces the following new features and changes:

- [Display logo on participant's screen during a meeting](#)
- [Display network information for the content shared in a meeting](#)
- [Auto prioritization of audio and content share over video during web app meeting](#)
- [Default join method to web app](#)
- [Enhancements to virtual background and blur](#)
- [Accessibility improvements](#)

4.1.1 Default resolution for web app presentation

From version 3.7.1, the maximum resolution for screen sharing is restricted to 720p. This implies that any participant, sharing presentation in a web app meeting will be restricted to 720p and cannot be modified. This will not affect the video resolution but only the content sharing.

Note: This change is not applicable for Safari browser.

4.1.2 Display logo on participant's screen during a meeting

From version 3.7, web app displays logos on the participants' screen. Organizations can use this feature for branding purposes by displaying their logos on the participants' screen during the meeting.

Logos are uploaded and configured in the Meeting Server. The administrators configure the logos to be displayed in certain positions on the participant's screen and web app renders them accordingly. Web app does not support adding or modifying logos. Depending on the position defined in the Meeting Server, logo is displayed in any of the following positions of the participants' screen:

- Left top
- Left bottom
- Right top
- Right bottom

Choose the Left top or Left bottom positions to prevent the logo from covering the participant count or the recording icon on the right-hand side of the web app or SIP screens.

Note:

- If the logo image is not uploaded in the Meeting Server or the customization license is not activated, the logo will not be rendered in the layout.
- This feature is supported on web app and SIP endpoints.
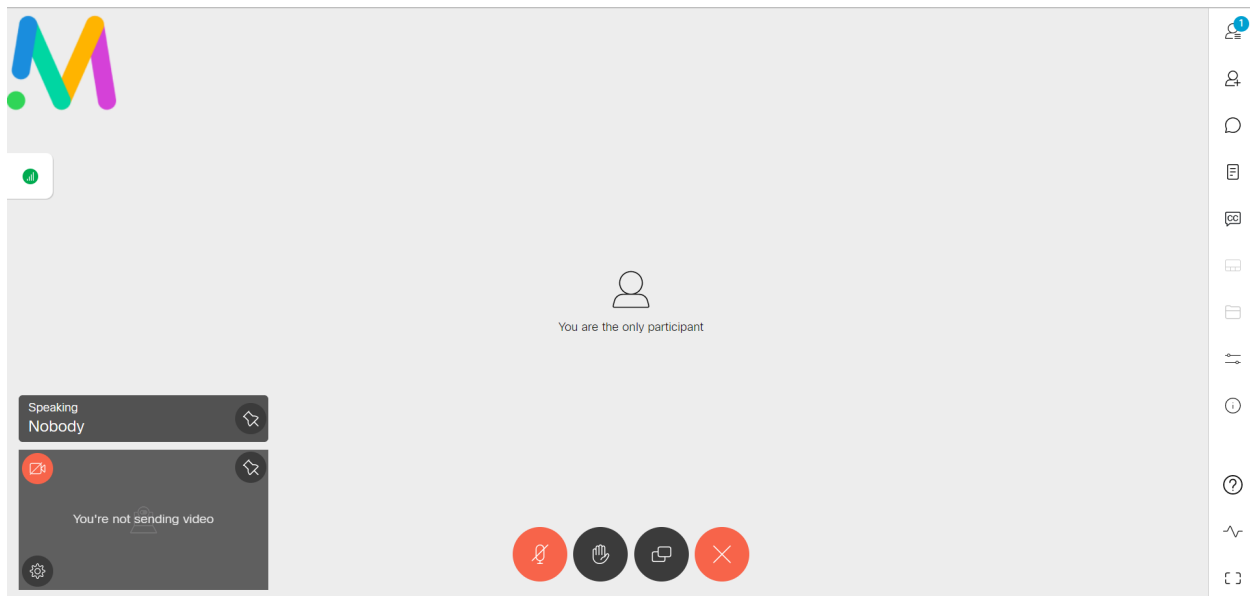
Logos can be rendered on custom and standard layouts. The logo position rendered will remain the same even if the user switches screen layouts.

Resizing the web app window will not affect the resolution of the logo. Web app renders the logo in its original size and position, as uploaded and configured on the server. However, the size and resolution of the logo are determined by the screen resolution of the participant/ endpoint.

Note:

- Logo will not appear on popped-out presentation window.

- While sharing content, the logo position on web app will remain as configured on the Meeting Server. However, the logo will be displayed in the video pane on SIP endpoints.

4.1.3 Display network information for the content shared in a meeting

Version 3.6 introduced the display of network statistics, during a web app meeting. Network statistics enables the web app participants to gauge whether they are experiencing a network, audio, or video issue during the meeting.

In version 3.7, this functionality is enhanced to improve its feature capabilities. Web app now shows network statistics for the content shared during the meeting. The audio, video, and content share metrics of an ongoing meeting is displayed in ⓘ **Call information** > **Media Health Statistics**.

∧ Media Health Statistics

☑ Mute notification

You are having the full meeting experience

	Send (kbps)	Receive (kbps)
Audio Metrics		
Jitter	10	4
Latency	30	30
Packet Loss	0%	0%
Codec Negotiated		
Video Metrics		
Latency	30	30
Jitter	10	4
Packet Loss	0%	0%
Video Resolution	6	10
Frames Per sec	80	80
Content Share Metrics		
Latency	30	30
Jitter	10	4
Packet Loss	0%	0%
Video Resolution	6	10
Frames Per sec	80	80

Note: Network health indicator, media and content share statistics are visible to web app participants only. SIP participants cannot view this.

4.1.4 Auto prioritization of audio and content share over video during web app meeting

Version 3.6 introduced the network indicator icons that notifies the web app participants about the network performance during a meeting. From version 3.7, web app monitors the network health and takes automatic actions to turn off/on the video and content share ensuring the best user experience in all scenarios of an unstable network.

Web app prioritizes audio over content share and video in all scenarios of unstable network. For example, if the network connection during a meeting is poor, web app automatically turns off the video. If the network continues to deteriorate, content sharing is turned off. Web app will always prioritize audio over content share over video and therefore, turns off the video, followed by content share, while retaining audio in all scenarios.

The network health is based on the jitter and packet loss metric values as shown below:

Statistics icon	Metric values	Health	Health messages/notifications
(green icon)	Jitter value is less than 30 ms and	Good	You are having the full meeting experience.
	Packet loss is less than 5%	From Poor/Bad to Good	You are having the full meeting experience. You may turn on the video.
(orange icon)	Jitter value ranging from 30 ms to 100 ms or Packet loss ranging from 5% to 15%	Poor	Issues may be limiting your meeting experience.
(red icon)	Jitter value is greater than 100 ms or Packet loss is greater than 15%	Bad	Meeting experience is being limited. The video has been disabled and currently in audio only mode.

As the network improves, web app restores content share and video in the same order of priority. Before taking any action of turning off/ on the video, web app monitors the network health status to ensure that it is in a steady state of good, poor, or bad for 45 seconds.

However, due to privacy considerations, web app does not turn on the participant's video (send video) automatically, but notifies them to turn on their video. The participants can enable their video back when the network is good.

Web app does not take any action if the meeting is in Audio Only or Presentation Only mode. However, web app will notify the participants regularly about the network health. If participants do not wish to see the network health status notifications, they can mute the notifications by selecting the **Mute notifications** check box in ⓘ **Call information** > **Media Health Statistics**.
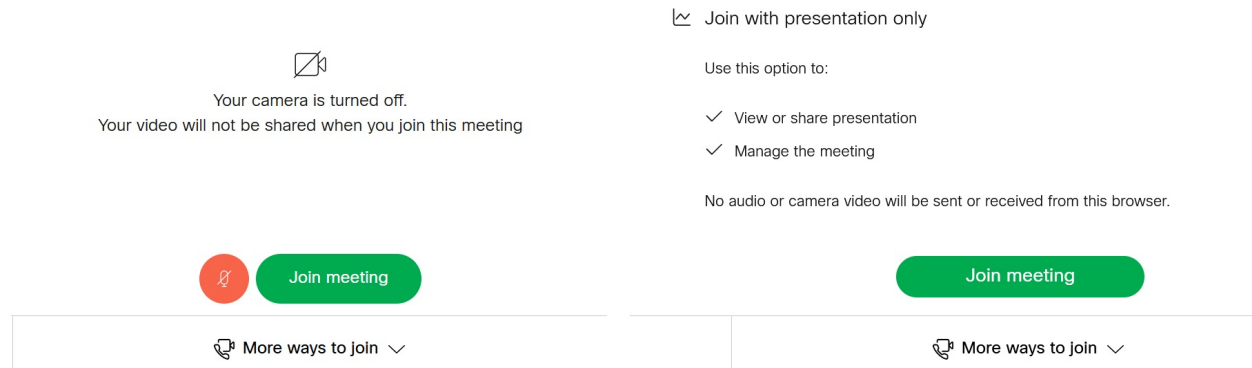
Note: Auto prioritizing is supported on web app only and is enabled by default. To disable this feature, contact the Cisco Meeting Server Administrator.

4.1.5 Default method to join web app meeting

In earlier versions of web app, the default method for the users to join a meeting was with audio and video mode. From version 3.7, the default joining method can be configured to **Audio and video** or **Presentation only** mode.

The system administrators configure the default join method in the Meeting Server for each user who may join the meeting, as a guest user using the meeting link or as space members using the **Join** button. Accordingly, the web app joining page for the participant defaults to **Audio and video** or **Presentation only** mode. If the default joining method is not configured in the Meeting Server, it defaults to **Join with audio and video**. Web app does not support configuring or modifying the configuration.

The default joining method can be set for each participant at various access levels. However, the participants can override the configured joining method by selecting the options listed under **More ways to join** in the web app joining options screen. The participants can change the joining method before joining the meeting and not during the meeting.

Your camera is turned off.
Your video will not be shared when you join this meeting

Join with presentation only

Use this option to:

✓ View or share presentation
✓ Manage the meeting

No audio or camera video will be sent or received from this browser.

Join meeting

Join meeting

More ways to join ⌄

More ways to join ⌄

Note: The default join method can be configured for web app participants only. Dial-in options are not configurable.

Any configuration changes in the API made during the meeting will not take effect on the participants who have already joined the web app meeting.

4.1.6 Enhancements to virtual background and blur

The virtual background feature enables web app participants to change their background with one of the available preset backgrounds, during a meeting. Version 3.7 gives administrators the ability to upload custom background images to the Meeting Server. Participants in the meeting can apply the custom backgrounds uploaded by the administrator.

Note:

- Custom backgrounds will appear in web app, if the administrator has enabled the feature and has uploaded the images in the Meeting Server.

- Web app participants cannot upload their own custom background images from/to web app.

Further, version 3.7 introduces support for blur and virtual background features on Microsoft Edge browser.

Operating System	Browser
Windows	Google Chrome, Mozilla Firefox, Microsoft Edge
macOS	Google Chrome, Mozilla Firefox, Microsoft Edge

4.1.7 Accessibility improvements

In version 3.7, web app supports the following accessibility improvement:

- Users can now use up or down arrow keys in the keyboard to navigate through chats in chat panel.

4.2 Using the web app

Web app allows you to join meetings with audio and video in a space. You can also share a screen or presentation in your meeting.

You can add or remove members to a space. You can also invite people both inside and outside of your organization to meetings.

Note: A space is a persistent virtual meeting room that a group of users can use at any time for a meeting. For more details refer to the Online Help or User Guide for web app.

You can use the web app on desktop, mobile or tablet from any of the supported browsers . See list of browsers for details.

Refer to the online help or User Guide for Cisco Meeting Serverweb app for detailed instructions on how to use the web app.

You can choose from the following options based on what you want to do:

- Sign in to the web app - You can sign in to web app, join meetings, view a list of all spaces you are a member of and view joining methods and copy the invitation details to invite someone to your meeting. You can create a space using pre-configured templates, edit or delete a space if you have appropriate permissions.

- Join a meeting - Use this option if you have been invited to a meeting. The invitation should include some details such as a meeting ID, passcode (optional), or a video address (URI).

- Schedule a meeting - To schedule a meeting, click Schedule meeting on the home page. Type a name and the select the space you want to use for the meeting. The meeting can be scheduled for one instance or to recur daily, weekly or monthly. You can add all the members of the selected space or add selected participants and configure their roles for the meeting.

4.3 Browser versions tested

Table 1 lists the browsers tested for web app at the time of release of a specific version of web app.

We always recommend using the latest version of browsers.

Note: Please note certain browsers such as Google Chrome and Mozilla Firefox automatically update to the latest version. The following table shows the version of browsers tested at the time of the official release of a version of Cisco Meeting Server. This means we have not tested this particular release with previous versions of those browsers.

We endeavor to test the latest maintenance release of each major release of Cisco Meeting Server against the latest public versions of all the browsers to keep them compatible and if we detect any issues we will endeavor to fix them as soon as possible.

Table 2:Cisco Meeting Server web app tested on browsers and versions

Browsers	Versions
Google Chrome (Windows, macOS, and Android)	111.0.5563.65
Mozilla Firefox (Windows)	110.0.1
Chromium-based Microsoft Edge (Windows)	110.0.1587.69
Apple Safari for macOS	16.3 (18614.4.6.1.6)
Apple Safari for iOS	16.3.1
Yandex (Windows)	23.1.5.708

Note: Web app is not supported on the legacy Microsoft Edge.

Note: Web app is not supported on virtual machines (VMs) running these supported browsers.

Important note for users using iOS 13 or later and macOS 10.15 or later

In order for users to be able to use web app on Safari on iOS 13 or later and macOS 10.15 or later, webbridge3 needs to be properly configured to comply with requirements stated here : https://support.apple.com/en-us/HT210176.

Users will not be able to open the app on Safari if these requirements are not met.

Important note about screen sharing on Chrome on macOS 10.15 or later

From macOS version 10.15 (Catalina) or later, to share the screen or application from the app running on Chrome, users need to enable permissions. Follow these steps:

1. From the Apple menu, open **System Preferences**.

2. Click on **Security & Privacy**.

3. Click on the **Privacy** tab at the top.

4. In the column on the left hand side, scroll down and click on **Screen Recording**.

5. Make sure Chrome is selected. Restart Chrome.

4.3.1 Important note about accessibility settings in Safari browsers

By default, Safari browsers do not allow navigation of UI elements via the 'Tab' key but via Option + Tab instead. This can be configured in Safari's Preferences as follows:

From your Safari browser menu, go to **Safari** > **Preferences** > **Advanced** > **Accessibility** > **Press Tab to highlight each item on a web page** to change your preference.

4.3.2 Important note about group policy settings in Microsoft Edge

If `WebRtcLocalhostIpHandling` - **Restrict exposure of local IP address by WebRTC** group policy is applied to Microsoft Edge browser, make sure to only use one of the following policy options:

- `AllowAllInterfaces` (default) or

- `AllowPublicAndPrivateInterfaces` (default_public_and_private_interfaces)

Any other option could cause connection issues.

4.4 Product documentation

The end-user guides such as User Guide, and visual 'How to' guides for web app are available in the following location:

https://www.cisco.com/c/en/us/support/conferencing/cisco-meeting-app/products-user-guide-list.html

5 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 and web app, 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.

5.1 Resolved issues in Cisco Meeting Server

Issues seen in previous versions that are fixed in 3.7.1

Cisco identifier	Summary
CSCwf17082	In rare cases, Meeting Server 2000 crashes when a guest user joins the meeting.
CSCwe88045	In rare cases, Meeting Server 2000 crashes while searching for cospace members in webapp and resulting in segmentation fault.
CSCwe67221	In rare cases, Meeting Server 2000 crashes while rendering fonts.
CSCwf59545	MaxQP H.264 encoder tuning.
CSCwd36402	When a SIP 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 3.7.

Cisco identifier	Summary
CSCwd40702	Jabber clients receive one way audio in meeting server conferences, after the meeting session gets refreshed (every 15 mins).
CSCwd16194	In rare cases, the Scheduler on 2000 fails to send email notifications, when using SMTP with Authenticated login configuration.
CSCvy61122	When users sign into web app and create a cospace, the domain name is not included in the video address.

5.2 Resolved issues in Cisco Meeting Server web app

The table below lists issues seen in previous versions that are fixed in 3.7.2

Cisco identifier	Summary
CSCwf87693	Unable to search or add users to spaces in Meeting Server 2000 with 240,000 users. Note: When scheduling a meeting in web app using a participant's email address, the user search may take longer.

The table below lists issues seen in previous versions that are fixed in 3.7.1

Table 3:List of resolved issues in 3.7.1

Cisco Identifier	Summary
CSCwf59540	In a web app meeting, when a participant shares their screen, the presentation is displayed (send) at a maximum resolution of 720p. **Note:** This change is not applicable for Safari browser.

The table below lists issues seen in previous versions that are fixed in 3.7

Table 4:List of resolved issues in 3.7

Cisco Identifier	Summary
CSCwd68381	When scheduling a weekly recurring meeting for a selected day, web app schedules the meeting a day after the intended date.
CSCwd35273	When searching for participant(s) to be added in a scheduled meeting, if the participant's name is typed incorrectly first and then corrected, web app doesn't show the participant's name in the search result. If an external user's email is typed in the participant's list of a scheduled meeting, the meeting is not created.
CSCwc76768	In a web app meeting, Audio and Video Statistics shows incorrect video frame rate in Firefox browser.
CSCwb60392	In a cospace meeting, if the presenter is moved to lobby while content is being shared, other participants in the meeting continue to see the content shared from the participant in lobby.

5.3 Open issues in Cisco Meeting Server

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
CSCwd06315	When a WebRTC user shares chrome tab with static content in a distributed call set up with SIP end points, SIP participants can intermittently see gray screen for few seconds and then restored.
CSCwd25525	CMS2K TLS syslog trust not working consistently
CSCwd36402	In a cospace meeting, if the SIP participant is moved to lobby while sharing the content, other participants in the meeting continue to see the content.
CSCwd89530	If the packet capture is not stopped gracefully using ctrl+C and the terminal is closed abruptly, further packet captures are not possible until CMS reboot.

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.
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.

5.3.1 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.

5.4 Open issues in Cisco Meeting Server web app

Table 5:List of open issues in 3.7

Cisco Identifier	Summary
CSCwc84546	After a presenter stops sharing their content and all participants in the meeting are inactive for a while but are still in the meeting, the participants are unable to see the content, even if the presenter resumes sharing the content.
CSCwe26144	When scheduling a meeting through the web app scheduler, if the participant's role is selected as "Role 1" (default), the participant cannot join the meeting using **Join** button.

Cisco Identifier	Summary
CSCwc23841	In a web app meeting, if a participant whose video is turned on and has applied blurred background, turns off the camera and switches it on later, a black background is displayed intermittently in place of the virtual background.
CSCwc76769	In Google Chrome browser, when a participant applies blur to their video and leaves the web app meeting, the camera is still on and does not close.
CSCwa17363	In web app, the participants who are moved to lobby from Meeting Management can see still the list of participants in the meeting even if they are waiting in the lobby.
CSCvz01888	If the role of a member was changed in the space before the meeting, a role change notification appears when the member joins the meeting.
CSCvu98805	Whilst in a meeting from web app on Firefox browser, if you open the presentation received in a second window, occasionally the content becomes non-responsive if the presenter stops and restarts the sharing or if another participant in the meeting starts sharing content at the same time. This is an issue with Firefox browser, for details see https://bugzilla.mozilla.org/show_bug.cgi?id=1652042. Work around: Maximize the second window or alternatively, close the presentation window and reopen it.
CSCvt71069	If the video layout 'speaker large' is selected, window does not re size correctly.

Appendix A: 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.

6.1 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.

6.2 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.

6.3 Call capacities

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

Table 6: Call capacities across Meeting Server platforms

Type of calls	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	30	175	218
Full HD calls 1080p30 video 1080p30/4K7 content	24	30	175	218

Type of calls	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	60	350	437
HD calls 720p30 video 720p5 content	96	120	700	875
SD calls 480p30 video 720p5 content	192	240	1000	1250
Audio calls (G.711)	2200	2200	3000	3000

Table 7 provides the call capacities for a single or cluster of Meeting Servers compared to load balancing calls within a Call Bridge Group.

Table 7: Meeting Server call capacity for clusters and Call Bridge groups

Cisco Meeting Server platform		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 2200	60 120 240 2200	350 700 1000 3000	437 875 1250 3000
	HD participants per con-ference per server	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	60 120 240 500	350 700 1000 1000	437 875 1250 1250
Meeting Servers in a Call Bridge Group	Call type supported				
	Load limit	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 7 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.

6.4 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 7.)

6.5 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 8.

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 8: 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.

6.6 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 7 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 8.

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.

Appendix B: Apps feature comparison

Feature comparison between Cisco Meeting Server web app and Cisco Meeting App for WebRTC.

Table 9:Feature comparison between Cisco Meeting Server web app and Cisco Meeting App for WebRTC

Feature	Web app 3.7	Web app 3.6	Web app 3.5	Web app 3.4	Web app 3.3	Web app 3.2	Web app 3.1	Web app 3.0
General								
Cisco Meeting Server version	3.7	3.6	3.5	3.4	3.3	3.2	3.1	3.0
Managing access for members	Yes	Yes	Yes	Yes	Yes	Yes	No	No
User-level permissions (e.g. can create [[[Undefined variable Brand-ingTypeVari-ables.coSpace_initial_ cap]]])	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Support for localization	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Branding	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Online help	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Encryption	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Single sign on	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Arabic language support	Yes	Yes	No	No	No	No	No	No
Join using video address (URI)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Schedule a meeting								
View list of scheduled meeting	Yes	Yes	Yes	Yes	Yes	No	No	No
Schedule a meeting	Yes	Yes	Yes	Yes	Yes	No	No	No
Modify a scheduled meeting	Yes	Yes	Yes	Yes	Yes	No	No	No
Delete a scheduled meeting	Yes	Yes	Yes	Yes	Yes	No	No	No

Feature	Web app 3.7	Web app 3.6	Web app 3.5	Web app 3.4	Web app 3.3	Web app 3.2	Web app 3.1	Web app 3.0
Space Management								
Space member roles	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Create / edit [[[Undefined variable BrandingTypeVariables.co Space_initial_cap]]]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Activate newly pro-visioned spaces	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Add / edit / delete space members	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Directory look up for Add Members feature	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
View information for [[[Undefined variable Brand-ingTypeVari-ables.coSpace_initial_ cap]]]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Send invitation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audio and video								
Audio	OPUS	OPUS	OPUS	OPUS	OPUS	OPUS	OPUS	OPUS
Video	H.264, VP8	H.264, VP8	H.264, VP8	H.264, VP8	H.264, VP8	H.264, VP8	H.264, VP8	H.264, VP8
Mic/camera configuration controls	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Blur your background	Yes	Yes	Yes	Yes	No	No	No	No
Virtual background	Yes	Yes	No	No	No	No	No	No
Far end camera control	Yes	Yes	Yes	Yes	No	No	No	No
Auto prioritization of audio and video	Yes	No	No	No	No	No	No	No
Screen share								
Content magnification	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Reset content zoom	Yes	Yes	Yes	Yes	Yes	No	No	No
View screen share	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Feature	Web app 3.7	Web app 3.6	Web app 3.5	Web app 3.4	Web app 3.3	Web app 3.2	Web app 3.1	Web app 3.0
Desktop sharing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Application sharing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
View screen share in a new window	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Re-size the video pane	Yes	Yes	Yes	Yes	Yes	No	No	No
Share content audio	Yes	Yes	Yes	No	No	No	No	No
Chat								
Chat	Yes, in call only	Yes, in call only	Yes, in call only	Yes, in call only	Yes, in call only	Yes, in call only	No	No
In-call								
On-screen messages	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Full-screen view	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Layout control	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Name labels	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Recording	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Streaming	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Active speaker label (Beta support)	Yes	Yes	Yes	Yes	Yes	No	No	No
Self-view	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Pin self-view	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mirror self-view	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Move self-view	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
HD/SD selection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Pin presentation preview	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Move presentation preview	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Meeting notes	Yes	Yes	Yes	Yes	No	No	No	No
Closed captioning	Yes	Yes	Yes	Yes	No	No	No	No
Share files	Yes	Yes	Yes	No	No	No	No	No

Feature	Web app 3.7	Web app 3.6	Web app 3.5	Web app 3.4	Web app 3.3	Web app 3.2	Web app 3.1	Web app 3.0
Network health indicator and media statistics	Yes	Yes	No	No	No	No	No	No
Content share metrics	Yes	No	No	No	No	No	No	No
Logo support	Yes	No	No	No	No	No	No	No
Participants								
Move participant	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Add participant	Yes (SIP only)	Yes (SIP only)	Yes (SIP only)	Yes (SIP only)	Yes (SIP only)	Yes (SIP only)	Yes (SIP only)	Yes (SIP only)
Remove participants	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Admit participants to a locked meeting	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Change a participant's role	Yes	Yes	Yes	Yes	Yes	No	No	No
Make participant important	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mute/Unmute other participants' audio and video individually	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mute/Unmute all participants' audio and video	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Send diagnostics during a meeting	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Send invite	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
View call info	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Mic / Camera controls during call	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Raise hand	Yes	Yes	Yes	Yes	Yes	No	No	No
Move call								
Use this device for screen share and call management only (while another device is used for audio and video)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Note: You cannot move a call to an external endpoint or move the audio to a regular phone during a call.

8   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

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)