Cisco Meeting Management

Cisco Meeting Management 3.5

(Build 3.5.0.29)

Release Notes

April 20, 2022

Contents

Document Revision History

Table 1: Document revision history

Date	Description
2022-04-20	Document published.

1 Introduction

Cisco Meeting Management is a management tool for Cisco's on-premises video meeting platform, Cisco Meeting Server. You can use the tool to monitor and manage meetings that are running on the platform, and it also provides information about which Cisco licenses you are using.

Meeting Management, with its current feature set, is included within existing Cisco Meeting Server licensing.

If you combine Meeting Management with Cisco TMS (TelePresence Management Suite), you can both schedule and manage meetings that are run on your Meeting Server Call Bridges.

These release notes describe new features, improvements, and changes to Cisco Meeting Management.

1.1 The software

Meeting Management is a virtualized appliance. Specifications of the VM (virtual machine) depend on how many simultaneous actions your Meeting Management has to perform or observe. See the *Installation and Configuration Guide* for specifications and requirements, including our estimates on sizing related to the number of Call Bridges you are managing.

For security, there is no user access to configuring via the console after first run. Except for the installation process, all use of Meeting Management is via a browser interface.

1.2 Upgrading from previous version

Before you upgrade:

- Please make sure you have an up-to-date backup of your Meeting Management.

  See the *Installation and Configuration Guide* for instructions.
- Check that your deployment meets the requirements of the version you are upgrading to.
- Plan your upgrade so no important monitored meetings are taking place while you are performing the upgrade.
- Notify other users before you start upgrading.

Note: All users, both video operators and administrators, will be signed out without warning, and data for ongoing and recent meetings will be lost when you upgrade.

- Make sure that you are ready to upgrade all connected Meeting Servers immediately after you upgrade Meeting Management. To avoid any issues caused by an older version of Meeting Management, we strongly recommend that you first upgrade Meeting Management, then upgrade the connected Meeting Servers.

To upgrade Meeting Management:

1. Sign in to the download area of cisco.com
2. Download the upgrade image file and save it in a convenient location.
3. Sign in to Meeting Management.
4. Go to the **Settings** page, **Upgrade** tab.
5. Click **Upgrade**.
6. Click **Upload upgrade file**.
7. Select the upgrade image file and click **Open**.
8. Check that the checksums are the same as the ones listed below, then **Confirm**.

   If the checksums do not match, do not install the upgrade, as the file may have been corrupted.
9. **Restart** Meeting Management to complete the upgrade.

1.3 Downgrading to previous version

If you need to downgrade to a previous version:

- Use the regular upgrade procedure and choose the image file for the appropriate version as the upgrade file.
- When using Reservation mode(SLR/PLR), ensure that you deregister from the reservation and then downgrade to a previous version. For more information on deregistering license reservation refer to Returning reserved licenses

1.4 Checksums for upgrade and installation files

Before you install or upgrade Meeting Management you should always check that the files have not been corrupted. See file names and checksums for this release below.

Upgrade image:

- Name of download file: `Cisco_Meeting_Management_3_5_0.zip`
- Name of upgrade image: `Cisco_Meeting_Management_3_5_0.img`
- MD5 checksum for upgrade image: `f34e95e6ae7ac3b87b9f58d716a51cbd`
- SHA256 checksum for upgrade image:
  `aefc5e841260cf72d7fcb197090825279f2cd5522be05e73a1ed1ea5eff6d3d2`
- SHA512 checksum for upgrade image:
  `5a1910ee065f57c1727eafa141fb4bbe8ff755e7f712bbfccf4a5f7759eb5aa54`
  `8de87beaf0f3af7a032c88bcc50d65e70144b5709a395fe27d243ac8e60b6ad`

OVA for new installation on vSphere 6.0 or below:

- File name: `Cisco_Meeting_Management_3_5_0_vSphere-6_0.ova`
- MD5 checksum for image: `c3ec0a450340ff160583a9443cccd8fe`
- SHA256 checksum for image:
  `b1daebce8a4f863073df557282816d3051a4f194115858163e0364183402c695`
- SHA512 checksum for image:
  `519c0a2cfb2d458b0b05f52cf826036035b42a68a0437d94360b4699706cbddfd3beecb18`
  `3a729503af59c586246e55a769018383665e768597ec580028f17e0`

OVA for new installation on vSphere 6.5 or later:

- File name: `Cisco_Meeting_Management_3_5_0_vSphere-6_5.ova`
- MD5 checksum for image: `62a16cd395de0c768da7f0017dc24682`
- SHA256 checksum for image:
  `0f7607ad19633685c8a6c96afc60a21e65550819ccd8929fe0d760c8a006ac04`
- SHA512 checksum for image:
  `461fc0e052786c32bd1faa22b40a57411e9802aa1cd9687e94477681c7d231eccd85db1d7`
  `22ca65fc51136109d5e5ff20dc0c65b373dba290d013915830621d7`

1.5 End of software maintenance for earlier versions

We support two full versions of Meeting Management at a time. This means that we give notice of end of maintenance and support for any given release when the subsequent two full versions have been released. For more information, see End of maintenance and support policy for Cisco Meeting Server, Cisco Meeting App and Cisco Meeting Management software.

1.5.1 End of software maintenance

Table 2: Timeline for End of Software Maintenance for versions of Meeting Management

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

1.6 Meeting Management and connected Meeting Servers must run the same software version

Meeting Management and connected Meeting Servers must run the same software version.

Before 3.0, every version of Meeting Management supported the same Meeting Server as well as the two previous ones. From 3.0, each Meeting Management version only supports Meeting Servers running the same version.

Note: To avoid any issues, we strongly recommend that you always upgrade Meeting Management before you upgrade the connected Meeting Servers. We have edited Upgrading from previous version to reflect this change.

2 New features and changes

In this section you can see what is new in 3.5.

2.1 Specify DTMF digits when adding a participant

Meeting Management now allows video operators to input DTMF digits while adding participants or another audio bridge, if DTMF digits are required. The DTMF digits are sent to the remote end by Meeting Server. When a participant or an audio bridge is added to a meeting, an audio prompt asks the operator to input the DTMF digits to enter the meeting. Adding commas in the DTMF digits add a pause between digits.

The video operators can provide the DTMF digits while adding a participant or an audio bridge using the **Add participants** option. The operator can also input the DTMF digits by clicking the **Send DTMF** icon available for each participant in the meeting list. On clicking the icon, a pop-up allows operator to enter the DTMF digits for the selected participant or space.

2.2 Taking snapshots of participants in a meeting

Taking snapshots of participants in a meeting aids in monitoring the overall meeting experience or for any diagnostic purpose such as to check the layout being displayed at the participant end or to check the participant video quality. In a managed meeting, Meeting Management allows a video operator:

- to take snapshot of the video the participant(s).
- to take snapshot of the video of all the participants that is displayed on the participant's screen depending on the layout selected.

The captured snapshots are available in 1280*720 (Width * Height) pixel. Snapshot is a licensed feature and is supported in Smart based Specific License Reservation (SLR) mode and online licensing mode. It is activated only when a separate license is purchased.

Note: In this version of Meeting Management, taking snapshots of participants in a meeting is not implemented for Permanent License Reservation (PLR) mode.

Snapshot icon will be available against each participant in the meeting list. Following options are available for capturing snapshots:

- **Incoming** (from participant to Meeting Server)- By default this option is selected and displays the snapshot of the participant.

- **Outgoing** (from Meeting Server to participant)- It displays the snapshot of video sent from Meeting Server to participant. This can be used to verify the layout displayed on the participant screen.
- **Incoming / Outgoing**– In this case, snapshot will be available for both the directions. Left window will display the incoming snapshot of a selected participant and right window will display the outgoing snapshot of participant screen.
- **Refresh** - **Refresh** button ↻ allows video operator to take a fresh snapshot of the option that is already selected.

Note: Due to security and privacy considerations, snapshot of content being shared in the meeting are not captured.

2.3 Automatic join for blast dial participants

In previous release, a new audio prompt **Press 1 to enter the meeting or * to hang up** was introduced to guide the participants with DTMF key options to accept or reject the call. From version 3.5, Meeting Management allows the blast dial participants to join the meeting immediately without having to input the DTMF keys. For meetings where participants must join immediately or if the participants cannot respond using the DTMF keys, the Meeting Management administrators can disable the audio prompt. The Meeting Management administrator can turn the audio prompt on or off both at the global level and at the participant level.

If the audio prompt is disabled at the global level, the audio prompt is disabled for all the participants in the blast dial list. Enabling or disabling the audio prompt at global level overrides the setting at the participant level. Administrator can then change the setting for individual participant if needed using the 📣 icon.

If the audio prompt is disabled, only the prompts **Hello, you are invited to enter the Cisco meeting** and **You are entering to the meeting now** are played. The audio prompt **Press 1 to enter the meeting or * to hang up** will not be played and the participant need not press the DTMF keys. They enter the meeting when they accept the call.

Note: Meeting Management stops redialing when call Decline or End call is received from remote end. In some cases, if due to network latency, these messages are not propagated to Meeting Server (For example: during PSTN calls), Meeting Management will continue to redial the participant until it reaches the maximum number of retries configured by the administrator. In such scenarios, it is recommended to enable the audio prompt so that the participant can enter the * DTMF key when prompted, to decline the call.

Meeting Management allows the following options to enable or disable the audio prompt:

- Using **Require prompt to connect participants** option available at a call level.
- Using **Require prompt to connect participants** option available when adding a dial-out contact.
- By clicking the audio icon 📢 available against each participant in the contact list.
- Using **CSV** button to add a .csv file. The values **On** or **Off** must be provided in the audio prompt column.

Note: The audio prompt value provided in the .csv file is case sensitive and will be disabled by default if an invalid value is entered or left blank.

2.4 Include 90 day license report in Meeting Management log bundle

Meeting Management logs now includes 90 day license report to provide visibility on customers' licensing usage to the support team, without having them to join a Webex meeting. The support team can then parse the 90 day license report and notify the customers of any necessary changes to the licenses.

From the **Logs** page **CMM logs** tab, you can download log bundle for Meeting Management using **Download log bundle** button. Downloaded log bundle now includes licensing reports in the .zip file.

2.5 Move participant to lobby

In previous release of Meeting Management, the video operators could move specific or all participants to lobby during a meeting using the **Move to Lobby** option. Version 3.5 includes an enhancement to this feature. If the Meeting Server administrator has allowed a participant to directly enter a locked meeting without waiting in the lobby, the video operator cannot move such participants to lobby. Such participants will have ⓘ icon placed against their name in the participants list. Hovering on the icon displays a tool tip **This participant can not move to lobby.** When the video operator tries to move such participants to lobby, a notification **Some of the participants cannot be moved to lobby** is displayed. For such participants the Move to lobby 👤 icon available against the participant is disabled.

2.6 Accessibility improvements

In version 3.5, Meeting Management introduces the following accessibility improvements:

- All the options on the Meeting Management **Licenses** page are now accessible through keyboard including the graphs.
- Users can now use **Esc** key to close the dialog box and return to previously active screen.

- In **Overview** page, user can now use the close button (**X**) to close the **Notifications** dialog box using the keyboard.
- The following elements in the Meeting Management now have meaningful description to help participants who use screen reader:

  - Meeting Management UI options such as Clear all button, Close button, Times link, Back button, Pin button and Edit button.

  - **Meetings** page options such as **Scheduled** or **Unscheduled**, **Active**, **Upcoming** or **Ended**.

  - Meeting search criteria drop-down list on the **Meeting** page.

  - all the options available on the **Licenses** page.

  - all the tabs available on the **Overview** page.

  - the options available on **Profile Menu**.

  - the dialog boxes and toggle buttons in **Blast dial configuration**, **User Profile** and **Settings** pages.

  - expanded/collapsed properties of button.

2.7 Online help

The online help has been updated according to changes that have been implemented for this trial release. Find it here:

https://meeting-infohub.cisco.com/olh/meeting-management/3-5/

3 Bug search tool and resolved and open issues

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

3.1 Using the bug search tool

1. Using a web browser, go to the Bug Search Tool.
   (https://bst.cloudapps.cisco.com/bugsearch/)
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 Management`, then in the **Releases** field select **Fixed in these Releases** and type the releases to search for, for example `3.5`.
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 Resolved Issues

4.1 Resolved in 3.5 (Build 3.5.0.29)

Reference	Issue
CSCwb13206	After upgrading to Meeting Management 3.4 if you take a backup of Meeting Management, the **License** page does not display the status of the license.
CSCwa36281	After restoring Meeting Management from a backup, when license mode is changed from **No licensing** to **Smart licensing**, administrator is unable to view Smart licensing screen and an error message **Could not fetch licenses please refresh** is displayed. When taking the backup, license mode was selected as **Smart licensing** and license status was **deregistered**. This issue is resolved when the administrator upgrades Meeting Management with the same build.

5 Open issues

The following are known issues in this release. If you require more details on any of these please contact Support, https://www.cisco.com/support.

Reference	Issue
CSCwa37575	License registration fails when the generated SLR code has more than one customization license. After generating SLR code which has more than one customization license, uploading the authorization code in Meeting Management displays an error message **There is some issue with Authentication file**. Refreshing the page shows status of Meeting Management as registered, but in **Licenses** tab it still displays status as **Unlicensed**.
CSCwa44321	When collecting logs for servers on the **CMS Log Bundle** tab, if administrator searches the servers by their name and selects multiple servers, only a single server stands selected.
CSCvz30358	In Meeting Management, while using Installation Assistant to add or configure a new Meeting Server, user can click the disabled **Next** button in several panels to move to the next panel without configuring the mandatory parameters.
CSCvt64327	If an administrator uses special characters in a template name, then these may appear differently in status messages, displaying escape characters instead.
CSCvt64329	For meetings hosted on Meeting Server 2.9 and later the lock button looks like it is enabled for gateway calls, although it has no effect. The Meeting Server ignores the lock status. Workaround: There is no workaround but we do not expect that participants would want to lock gateway calls.
CSCvt64330	If you are using Smart Licensing and move a Meeting Management deployment to a different virtual account, then the information will not be updated in its user interface. Workaround: Manually renew registration now.
CSCvt00011	If the connection to one of the Call Bridges in a cluster is lost, then Meeting Management may not receive details about the space a meeting takes place in, and streaming may not work.
CSCvr87872	If CDRs are lost, Meeting Management may not reflect changes for participants who need activation. For instance, Meeting Management may keep displaying participants in the lobby when they have already been activated and moved to the meeting.
CSCvq73184	The user interface does not indicate that you cannot turn pane placement off if it is turned on for the space where the meeting takes place.

Note: Due to macOS updates, some certificates will no longer work for macOS users using Chrome. You should check that your certificate complies with the requirement "TLS server certificates must contain an ExtendedKeyUsage (EKU) extension containing the id-kp-serverAuth OID."

6 Interoperability

Interoperability test results for this product are posted to http://www.cisco.com/go/tp-interop, where you can also find interoperability test results for other Cisco conferencing products.

6.1 Mute/unmute and layout behaviors

For more information on endpoint mute/unmute and layout control behaviors when used with Meeting Server and managed by Meeting Management, see:

- How will my endpoint mute/unmute controls behave when used with Cisco Meeting Server and managed by Cisco Meeting Management?
- How will my endpoint layout controls behave when used with Cisco Meeting Server and managed by Cisco Meeting Management?

7 Product documentation

The following site contains documents covering installation, initial configuration, and operation of the product:

https://www.cisco.com/c/en/us/support/conferencing/meeting-management/tsd-products-support-series-home.html

7.1 Related documentation

Documentation for Cisco Meeting Server can be found at:

https://www.cisco.com/c/en/us/support/conferencing/meeting-server/tsd-products-support-series-home.html

Documentation for Cisco Meeting App can be found at:

https://www.cisco.com/c/en/us/support/conferencing/cisco-meeting-app/tsd-products-support-series-home.html

Accessibility Notice

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

The Voluntary Product Accessibility Template (VPAT) for Cisco Master Project 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

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)