



Cisco Meeting Management

Release 3.8

(Build 3.8.0.21)

Release Notes

September 08, 2023

Contents

Document Revision History	3
1 Introduction	4
1.1 The software	4
1.2 Upgrading from previous version	4
1.3 Downgrading to previous version	6
1.4 Deploying the OVA	6
1.5 Checksums for upgrade and installation files	6
1.6 Smart Licensing	7
1.7 End of software maintenance for earlier versions	7
1.7.1 End of software maintenance	7
1.8 Meeting Management and connected Meeting Servers must run the same software version	8
2 New features and changes	9
2.1 Enhancements in license reservation	9
2.2 Assigning spaces to video operators using Meeting Management	9
2.3 Accessibility improvements	11
3 Bug search tool and resolved and open issues	13
3.1 Using the bug search tool	13
3.2 Resolved Issues	13
3.3 Open issues	14
4 Interoperability	16
4.1 Mute/unmute and layout behaviors	16
5 Product documentation	17
5.1 Related documentation	17
Accessibility Notice	18
Cisco Legal Information	19
Cisco Trademark	20

Document Revision History

Table 1 : Document revision history

Date	Description
2023-09-07	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.

Upload keys to verify upgrade images:

Cisco Meeting Management embeds a signature within the upgrade image which Meeting Management uses to confirm whether or not the image is genuine.

Image signatures are only verified when upgrading from a signed image. So manual verification is still advised when upgrading from an unsigned image to a signed one. i.e. if you upgrade from 3.6 to 3.7, or downgrade to earlier versions, you are still advised to manually verify the hashes. This feature will be fully effective when upgrading from 3.7 and beyond.

From version 3.7, upgrading to a special build will require uploading a special key. The **Upload Key** button is introduced to enable administrators to upload the public key and verify the upgrade images. However, the administrators will perform this action only when upgrading to a special build.

To upload public keys:

1. On the **Settings** page, go to **Upgrade** tab.
2. Click **Upload key** then browse and select the public key. The selected public key is verified and uploaded.

Note: Upgrades from a signed production/ special build to another signed production build will not require any action from the administrator. Meeting management verifies the upgrade images automatically without the need for manual verification of the hashes.

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 Deploying the OVA

When uploading OVA to Vcenter and deploying, the Publisher field should show (Trusted certificate). If you see a warning for an invalid certificate and not- trusted cert when importing the OVA, see this article: <https://kb.vmware.com/s/article/84240>. You may have to add the intermediate and root certificates corresponding to the certificate used to sign the OVA, to the VECS Store. To procure intermediate or root certificates or any other issues, contact [Cisco Technical Support](#).

1.5 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_8_0.zip`
- Name of upgrade image: `Cisco_Meeting_Management_3_8_0.img`
- MD5 checksum for upgrade image: `1cf2f7e9c173f61a809a1d47499d12b5`
- SHA256 checksum for upgrade image:
`b1d152bbc37f8b48fe902c929b0b5a762c558f8e4b329ef3587950773a2abe4a`
- SHA512 checksum for upgrade image:
`84fe0bea3926befbd541a2eae31dec89e5ef46a0f3695e951ae0833097f376c14717429049d0bb67df1218972d128977579635ab7f046f9ad77f63a4938ef96e`

OVA for new installation on vSphere 7.0:

- File name: `cisco_Meeting_Management_3_8_0_vSphere-7_0.ova`
- MD5 checksum for image: `c12fbee54c4788b048a8407ddc1efc5b`
- SHA256 checksum for image:
`a73ba42163a41528298954c003a126d31f93e08b16a369f507f0d74df67b387e`
- SHA512 checksum for image:
`116c8ccb8b67c4b2f682160cf2707abcfb9aa98f60aca9ae133b2745b54a20b79f29cd31b
f142c7d7e392b7ef175aa3096fd1a79e3230225cd9fad24a943b35e`

Note: VMware has discontinued support for ESXi 6.x versions and Meeting Management will no longer be tested in any of the 6.x versions. This release of version 3.8 supports ESXi 7.0.x only. Support for Esxi 8.0 will be added in upcoming releases.

1.6 Smart Licensing

From the 3.4 release onwards, Smart licensing is mandatory for Meeting Management. 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, see [Cisco Meeting Management User Guide for Administrators](#).

1.7 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](#).

1.7.1 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 3.5.x	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes for Cisco Meeting Management version 3.5.x is July 15, 2023.

1.8 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 3.8.

2.1 Enhancements in license reservation

Meeting Management uses License reservation to activate features and reserve licenses. From version 3.8, while reserving a license in the **Licensing** section, if Cisco Smart Software Manager (CSSM) takes more time than the expected 30 seconds to respond, two more retries will be attempted with varying timeout values. Meeting Management waits for 60 seconds and 90 seconds for second and third retry respectively. If license reservation is unsuccessful after three retries, **Overview** page of Meeting Management displays **Unable to reach Cisco Smart Software Server**. Users can then reinitiate the license reservation procedure and the message will be cleared after the licenses are successfully reserved.

From this release, the Licensing reports downloaded using **Download log bundle** button in **CMM logs** tab in **Logs** page will include the number of attempts or retries made for license reservation.

2.2 Assigning spaces to video operators using Meeting Management

From version 3.8, Meeting Management administrators can tag video operators to specific spaces, giving them access to the meetings associated with those spaces only. Previously, Meeting Management video operators had access to all spaces and meetings. Administrators can now limit this by adding tag(s) while creating or modifying video operators allowing them to manage and monitor the meetings more effectively.

In this feature:

- Each space can have a single tag. However, the same tag name can be added to multiple spaces. Administrators can then assign this tag to video operators, providing them access to appropriate space or meeting. Tag name may contain up to ten characters and is case-insensitive. It can be created in Meeting Server only, using the coSpace API.
- A video operator can be given access to multiple spaces and meetings by assigning multiple tags. A video operator can be assigned a maximum of 10 tags.
- Space tags can be added to both new and existing video operators. If video operators are not assigned any tags, they will have access to all the spaces or meetings (with or without tags). Similarly, meeting spaces that do not have tags will be visible to operators who do not have any tags assigned.
- Tags added or modified for a space during an ongoing meeting will reflect only from the subsequent meeting.

- Tags added or modified to video operators while they are signed in to Meeting Management, will reflect only after the video operator signs in for the next session.
- Meeting Management administrators can view all the meetings and spaces (with or without tags) using the **Meetings** or **Spaces** tab respectively. Tags cannot be added to Meeting Management administrators.
- Video operators will only be able to move participants to the meetings held in the spaces they are tagged to.
- The usernames for administrator and video operator must be unique.
- It is recommended to use different usernames for both Local and LDAP user group to avoid the tags from being assigned incorrectly.
- On removing/disconnecting any LDAP user group from Meeting Management and then adding it back, Meeting Management continues to retain the tags assigned by the administrator to that LDAP user group.

Follow these steps to add tags for a new video operator:

1. On the **Users** page, in **Local** tab, click **Add Local User** button to launch **Add Local User** pop- up window.
2. In the new **Add tags** field, enter the tags to be assigned. Add tag(s) corresponding to the space(s) in the new field. A maximum of ten tags can be allotted for a video operator.

Add Local User [X]

Details

Username

First name

Last name

Role

Administrator Video operator

Password

New password

Confirm password

Add tags

[Remove all](#)

You can add up to 10 tags

Follow these steps to add tags for the existing video operators and LDAP user groups:

1. On the **Users** page, in **Local/ LDAP user groups** tab, scroll down to find the video operator for assigning space tags.
2. Click **View User Profile** button available in **Actions** against the selected video operator to launch **User Profile** pop- up window.
3. Click **Edit** button in **Add tags** field.

4. Add tag(s) corresponding to the space(s) in **Add tags**. A maximum of ten tags can be allotted for a video operator.
5. Click **Done**.

2.3 Accessibility improvements

In version 3.8, Meeting Management introduces the following accessibility improvements:

- All the radio buttons in Meeting Management can be navigated using **Arrow** keys.
- The tool tip/help tip buttons in the **Licenses** page opens text only when clicked.
- Keyboard users can navigate between the options in **Local/Admin** menu on the top right using the **Arrow** keys.
- When the user tab to **Overview** option in the left side, they are now able to use **Arrow** keys to navigate through all the tabs.
- All the headings are now in logical hierarchy in **Overview** page.
- In **Smart licensing** option in **Overview** page, focus now moves inside the date picker only when user presses **Tab** key, after pressing **Enter** key used for opening the date picker.
- While using screen reader, when the user presses **Enter** key to navigate to various options in the **Licenses** page, all the options can be activated.

- In **Overview** page, when the user presses **Done** button in the **Notifications** dialog or **Esc** button, the focus is back to **See notifications** button.

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/). (<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.

3.2 Resolved Issues

Resolved in 3.8 (Build 3.8.0.21)

Reference	Issue
CSCwd60705	PMP/SMP Smart license allocation takes more than 5 minutes to complete.
CSCwe34764	While recording a meeting from Meeting Management, the recording button spins if the meeting participants are distributed across various call bridges.
CSCwe53152	During a meeting, Lync participants are unable to take their (own video) snapshots when any of the participants share their screen.

3.3 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
CSCwh48492	While entering text data in Title and Body fields in Sign in messages section in Settings tab, focus is lost from the input field.
CSCwe65616	Taking snapshots is only allowed on CMM for a licensed snapshot version. For the unlicensed version, it returns an error message.
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."

4 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.

4.1 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?](#)

5 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>

5.1 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.

© 2023 Cisco Systems, Inc. All rights reserved.

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)