Cisco Meeting Management

Cisco Meeting Management 3.1.0

(Build 3.1.0.70)

Release Notes

November 30, 2020

Contents

Document Revision History

Table 1: Document revision history

Date	Description
2020-11-30	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 <u>below</u>, 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.

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_1_0.zip`

- Name of upgrade image: `Cisco_Meeting_Management_3_1_0.img`

- MD5 checksum for upgrade image: `fd2e9189e3b4977a03a4abb3d53edbe6`

- SHA256 checksum for upgrade image:
  `11305938ff5e8c1bce16646fd9018aaf22bea36d1e026010ccb95b48f1b864b3`

- SHA512 checksum for upgrade image:
  `4630cdb5d0ca2f2f0e821f820b2b2847726f76cb874b08629ad31c2bfe49670e81cbbabce`
  `74f543be9b776b2055fa6f432a4ddaba79d2ab1f12f752bb77d84a4`

OVA for new installation on vSphere 6.0 or below:

- File name: `Cisco_Meeting_Management_3_1_0-vSphere-6_0.ova`

- MD5 checksum for image: `8aa838847cb2304e3b1837214c990abc`

- SHA256 checksum for image:
  `a7895091f394e21a909ba6f18c1e0d2cfd462535c1d760d6748879a187ef7f06`

- SHA512 checksum for image:
  `16567984d2ed9be5dd53e803bdb0595e5273dea0c90d30d1585ce84ab3cf653e7a73f03cb`
  `9fd4720c355582a217e057165c4b12ff944cbb1128190e3ee79f2e9`

OVA for new installation on vSphere 6.5 or later:

- File name: `Cisco_Meeting_Management_3_1_0-vSphere-6_5.ova`

- MD5 checksum for image: `9b8079232c1e020eed0b1d26a7653196`

- SHA256 checksum for image:
  `063861bd9a5901af8529d4af4808795c93be39eb69abf5f66c483716183ffe04`

- SHA512 checksum for image:
  `255f96ce77a07014d0c95c79dc098e755e27ea30bc539371736c9b66796a08657ce757b1a`
  `365af7a14e03311315fa538c8fa5e32a459798c2e18c49369fb71e7`

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

On release of Cisco Meeting Management 3.1, Cisco announces the timeline for end of software maintenance for version 2.9.

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

Cisco Meeting Management version	End of Software Maintenance notice period
2.9	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes for Cisco Meeting Management version 2.9.x is March 1, 2022.

2 New features and changes

In this section you can see what is new in 3.1.

2.1 Provisioning update: Choose a name for each user import

In this release, you can enter a name for each user import. If you do not enter a name, Meeting Management will create a name based on its configuration.

See the *User Guide for Administrators*.

2.2 Provisioning update: Choose who can create which types of spaces

In previous releases, you could make templates available to all web app users for creating spaces. In this release, you can assign specific templates to specific users.

See the *User Guide for Administrators*.

2.3 Provisioning update: Define minimum password length for each participant role

Previously, the Meeting Server's default settings would always be in place. In this release, you can choose to use the default setting, or you can define a minimum password length for each participant role.

See the *User Guide for Administrators*.

2.4 Provisioning update: Automatically create spaces for users

In this release you can provision spaces for users.

See the *User Guide for Administrators*.

2.5 Provisioning update: Schedule Meeting Server LDAP sync

In previous releases, you could manually trigger an LDAP sync to implement changes to provisioning settings. Now you can also schedule LDAP sync to be performed at specific times each week.

See the *User Guide for Administrators*.

2.6 Improved labels for transmitting and receiving in the participant details

Many users provided incorrect information to Support because they were confused about the direction of transmitting and receiving. To make that clearer, we have changed the labels to **To participant** and **From participant**.

The User Guide for Video Operators has been updated to reflect the change.

2.7 Use Webex Control Hub to monitor your Meeting Management and Meeting Server deployments

You can connect your Meeting Management deployment to Webex Control Hub, so you can see Meeting Management alerts and metrics from the Control Hub interface. You can also set up email and Webex Teams notifications for alerts.

From Webex Control Hub you can:

- See status for all connected instances of Meeting Management
- See notifications from the Meeting Management overview page
- Set up email and Webex Teams notifications

For information and instructions, see https://meeting-infohub.cisco.com/olh/meeting-server-cloud-connector/

Note: This is a beta feature in Meeting Management 3.1.0, and it is not generally available in Control Hub and the Webex Cloud. If you want to test this features, contact your Cisco Account team or send an email to personalmultiparty@cisco.com.

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.

2.8 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.

2.9 Changes to requirements

We have updated the section to say that Meeting Management 3.1 is only supported with Meeting Server 3.1. We have also added that the only supported version of Smart Software Manager On-prem (satellite) is version 8-202008, and we have added Webex Cloud and Control Hub to port information.

For all requirements and prerequisites for Meeting Management 3.1, see the "Before you start" section of the *Installation and Configuration Guide.*

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 `3.0`.

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 3.1.0 (Build 3.1.0.70)

Reference	Issue
CSCvw14115	Local users that have been passed over from SSO proxy cannot sign in due to extra settings with the HTTP header request.
CSCvv78323	When Meeting Management had to process a large number of CDRs, its web interface could become unresponsive.
CSCvv65096	When you have chosen to only use manual configuration for IPv6 adresses, SLAAC is still being used. Workaround: Disable SLAAC at the router.
CSCvu96310	If Meeting Management was already registered to the Cisco Smart Software Manager before you upgraded to 3.0, then Meeting Management may not be able to reauthorize. Workaround: Change to No licensing mode, then change back to Smart Licensing mode.
CSCvu06383	Under some circumstances, Meeting Management includes dropped participants in the number of lobby participants displayed in the list of meetings.
CSCvu96309	There is an error connecting to Cisco Smart Software Manager On-prem. Workaround: Contact your Cisco sales representative for guidan

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
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.

© 2020 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)