Cisco Meeting Management

Cisco Meeting Management 2.9.0

(Build 2.9.0.67)

Release Notes

April 08, 2020

Contents

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 numbers 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.

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 in the release notes, 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_2_9_0.zip`**
- Name of upgrade image: **`Cisco_Meeting_Management_2_9_0.img`**
- MD5 checksum for upgrade image: **`dae7acfd221c7d74ec71603770f911aa`**
- SHA256 checksum for upgrade image:
  `a9eeca83ef1c64fb3c0ab785767348779ea52cd913256d24bdf1510969374dd6`
- SHA512 checksum for upgrade image:
  `41db7a47e6bb3c14ee2abdcdd8315fa2c1a6afd6f2707e2b4f37def90c8e6cb23cb5391342ec1d67e459885d1f597345887459059469fc0c164f671b59e910f9`

OVA for new installation on vSphere 6.0 or below:

- File name: **`Cisco_Meeting_Management_2_9_0_vSphere-6_0.ova`**
- MD5 checksum for image: **`15c0f8819a52e2ce6b4d1f59c497d442`**
- SHA256 checksum for image:
  `ddfe939a1cbceb4e1609d83af6f5a5838b97b9bb781af3eebb7ed044cb885f6a`
- SHA512 checksum for image:
  `d001d122f830354dff993abc4a807335d11136489dcb5ca3978a6e837414a94b9d8604e800451e819703a04476eb70dab1098177dc2b3f1cc71447d61e61914b`

OVA for new installation on vSphere 6.5 or later:

- File name: **`Cisco_Meeting_Management_2_9_0_vSphere-6_5.ova`**
- MD5 checksum for image: **`0a59844c65c761b41700f41af884f2d5`**
- SHA256 checksum for image:
  `979ad09a02e1e20e911e919d7fd2de7646c24db11287b34e1853354f64c45d8a`
- SHA512 checksum for image:
  `83b100761a7e7d59bab1cbb469e218fbfdabbcd31ac75a2265bb501f82e5b970becc8df8ba6946634d1985cc2d961293414f64f44ad95ed9a0bdcc07eb188eb5`

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 2.9, Cisco announces the timeline for end of software maintenance for version 2.7.

Table 1: Timeline for End of Software Maintenance for versions of Meeting Management

Cisco Meeting Management version	End of Software Maintenance notice period
2.7	4 months after first release of version 2.9

2 New features and changes

In this section you can see what is new in 2.9.

2.1 Events for mute status

Previously Meeting Management would get information about mute status via the Meeting Server API. In this release, the Meeting Management will get this information via events to improve performance. Video operators may notice this when they enter a large meeting or scroll through a long participant list.

2.2 Idle session timeout

Previously, users would stay signed in for up to 24 hours whether they were active or not. In this release you can decide whether users should be signed out if they are inactive, and you can set a specific time limit for how long users can be inactive before they are signed out.

See instructions in the *Installation and Configuration Guide*.

2.3 Connect LDAP servers to Cisco Meeting Servers and import users

Previously, LDAP mappings for importing users have been configured via the Meeting Server API. In this release, you can use Meeting Management to can enter LDAP server details and configure LDAP mappings from a **Provisioning** page which you can access from the **Servers** page.

See instructions in the *User Guide for Administrators*.

2.4 Create space templates for web app users

Previously, settings for spaces have all been configured separately via the Meeting Server API. In this release, Meeting Management lets you create space templates that consist of pre-configured settings that you make available for web app users so they can use them to create one or more different types of spaces. For instance, you can let them choose between a team space where all participants have the same privileges and a host and guest space where some participants are guests with limited privileges.

See instructions for administrators in the *User Guide for Administrators*. To know what users will see in the web app, see the *Cisco Meeting Server web app User Guide*.

2.5 Lock out all new participants

Previously, the meeting lock would only affect non-Activators (non-members who need activation to join a meeting). The lock still works like this for Meeting Server versions 2.8 or earlier.

For Meeting Server 2.9 we have implemented a new lock mode that makes the meeting lock affect all participants. This new lock mode is the default for Meeting Server 2.9.

Note: Meeting Management does not show which lock mode is in use.

Make sure that you inform your video operator if there are changes to the lock mode.

For instructions on how to use the meeting lock, see the *User Guide for Video Operators*. For more information about how the new lock mode works, see the *Cisco Meeting Server 2.9 Release Notes*.

2.6 Meeting lock for scheduled meetings

In the previous release, the meeting lock button was disabled for scheduled meetings. In this release, the meeting lock button is enabled for all scheduled meetings.

The *User Guide for Video Operators* had been updated to reflect this.

2.7 Admit all lobby participants

For meetings hosted on Meeting Server 2.9, the **Admit all** button will let all participants into the meeting, whether or not an Activator is present in the meeting.

For meetings hosted on Meeting Server 2.8 or earlier, the **Admit all** button will work as it did in previous releases.

The *User Guide for Video Operators* had been updated to reflect this.

2.8 Support for Cisco Meeting Server web app

In this release we have added a call type named web app, which is short for the Meeting Server web app.

For information about the new web app, see the *Cisco Meeting Server web app Important information* document.

2.9 CBC3 cipher suites no longer available

The following cipher suites are no longer available for Meeting Management:

- ECDHE-RSA-DES-CBC3-SHA;
- DES-CBC3-SHA

The *Installation and Configuration Guide* and the *User Guide for Administrator* have been updated to reflect this.

2.10 Changes to requirements

Meeting Management 2.9 supports Meeting Server version 2.7 or later. We recommend using version 2.9, which is required for admitting all participants, and for using the new lock mode.

For all requirements and prerequisites for Meeting Management 2.9, see 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 example **`2.6`**.
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 2.9.0 (Build 2.9.0.67)

There are no new resolved issues in this version.

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
CSCvt64466	Meeting Management can handle space template descriptions to maximum 255 bytes (255 characters if you are using Roman characters with no accents). This is much less than the Meeting Server limit of 1023 bytes. If a space template description of over 255 bytes is committed, either from Meeting Management or via the Meeting Server API, then Meeting Management does not display any provisioning pages. Workaround: Only commit space template descriptions that are shorter than 255 Roman characters, or 63 Chinese characters.
CSCvt64326	If an administrator attempts to enter more than one "$" in the **Unique URI generator** field while configuring a participant role, then Meeting Management will accept the setting, although the following LDAP sync will fail. Workaround: Only enter one "$".
CSCvt64328	If an administrator changes a space template from using unique URIs to using the same URI for all roles, then Meeting Management does not remove the URI generator. Workaround: Remove all roles, change the setting, then recreate the roles.
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 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.
CSCvs99792	If a user is looking at the meeting details for an active meeting, and another Call Bridge is added to the call, then Meeting Management does not receive Events for participants who are connected to the new Call Bridge. Workaround: Open participant details for any participant in the meeting or leave the meeting details view. When you return to the meeting details view, the page will be refreshed, and Meeting Management will receive all Events.
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.

Reference	Issue
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: The following known limitation has been reported by a customer:

- CSCvn09301: Meeting Management may occasionally send packets with a source address in the range reserved for documentation. This is a bug to a third-party component: https://github.com/moby/moby/issues/18630. As the impact to CMM is low, we will not be producing any internal fix.

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

Document Revision History

Table 2: Document revision history

Date	Description
2020-04-08	Document published.

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)