Cisco Meeting Management

Cisco Meeting Management 2.5.1

(Build 2.5.1.65)

Release Notes

January 17, 2019

Contents

1 Introduction

Cisco Meeting Management is a management tool for Cisco's on-premises video conferencing platform, Cisco Meeting Server. It provides a user-friendly browser interface for you to monitor and manage meetings that are running on the Meeting Server.

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.

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 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_5_1.zip`**
- Name of upgrade image: **`Cisco_Meeting_Management_2_5_1.img`**
- MD5 checksum for upgrade image: **`287cad4142fa71054c71ed467ddfd7d3`**
- SHA256 checksum for upgrade image: **`b4496ba5e9cda115e4cc4be46e5fa92cf4d1e93a5d45b2b0ac39ae3200f7b9a4`**

OVA for new installation on vSphere 6.0 or below:

- File name: **`Cisco_Meeting_Management_2_5_1_vSphere-6_0.ova`**
- MD5 checksum for image: **`ca5f7c717aa11c6b27e767a08032a4a9`**
- SHA256 checksum for image: **`0f17e004a774bb7acae797fd4ec6d0bbc95ca79aba48129b87d23d1fae08a74d`**

OVA for new installation on vSphere 6.5 or greater:

- File name: **Cisco_Meeting_Management_2_5_0_vSphere-6_5.ova**
- MD5 checksum for image: **1306a003bfc618cd9cb08d9f7ff2cac3**
- SHA256 checksum for image: **43048c430b040c2745d8fff949b7c48311c4dbeb059a517bc1bd391c1b10ffb4**

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 for Meeting Management 1.0

On release of Cisco Meeting Management 2.5, Cisco announces the timeline for end of software maintenance for version 1.0.

Table 1: Timeline for end of software maintenance for version 1.0

Cisco Meeting Management version	End of software maintenance
1.0	4 months after first release of version 2.5

2 New features and changes

2.1 Version numbering aligned with Cisco Meeting Server

We have skipped from version 1.1 to version 2.5 to align with the Cisco Meeting Server version numbers.

2.2 Local users

In version 2.5 you can add both LDAP users and local users. Also, you can edit security policy settings for local users.

Local user accounts are useful for:

- Setup of Meeting Management
- In lab environments, for testing of Meeting Management
- In production environments, for making sure that you have access to Meeting Management if there are LDAP issues
- In production environments, for making changes to LDAP server details

Note: For general use in production we recommend that users are authenticated via LDAP.

Note: If you have both LDAP users and local users, you may need to tell your users if they should choose **LDAP** or **Local** as **Account location** when they sign in.

Note: A local administrator user account is generated during first time setup, see below. If you upgrade to 2.5 from a previous version, all local users must be added manually.

For more information, see the *Installation and Configuration Guide* or the *User Guide for Administrators*.

2.3 Persistent user account for setup

Previously, setup was done with a one-time password. In this version the credentials provided in the console is for a persistent local administrator user account. For security, you can change the credentials for this account as part of the first time setup.

The persistent account has eliminated the risk of being locked out after saving LDAP details, and the first time setup is easier.

The *Installation and Configuration Guide* has been updated to reflect the changes.

2.4 Fewer steps in the installation process

The persistent local user account has made it possible to skip the initial LDAP setup.

The *Installation and Configuration Guide* has been updated to reflect the changes.

2.5 Remote recording indicator in dual homed meetings

When a recording is not handled by the Meeting Server, such as when a Lync or Skype for Business participant is recording a dual homed meeting, the label **Remote recording on** will be displayed in the meeting details view.

For more information, see release notes for Cisco Meeting Server 2.4. For operator instructions, see the *User Guide for Video Operators*.

2.6 More than one label for scenarios with limited functionality

In the previous release, only one label would be displayed for special case scenarios. In this release, all relevant labels are displayed. For instance, if you have a dual homed meeting running on a Meeting Server with software version 2.3, you will see both the **Dual homed** label and the **Some features not supported by Meeting Server** label.

For operator instructions, see the *User Guide for Video Operators*.

2.7 Scheduled participants

In this release you can see a list of scheduled participants for upcoming meetings. The list is displayed as a checklist which you can use to check which participants have joined the meeting. Check marks can only be seen by the video operator who added them, and they are saved until this video operator is signed out.

For operator instructions, see the *User Guide for Video Operators*.

2.8 Pinning meetings from the meeting details view

You can now pin a meeting from the meeting details view as well as from the list view. The effect is the same; the meeting stays at the top of the list of meetings until you unpin it, or until you are signed out of Meeting Management.

For operator instructions, see the *User Guide for Video Operators*.

2.9 Local users restored separately from LDAP users

Before, all information from the **Users** page was stored together. In this version, information about local user accounts, including password history, is stored separately so you can restore local users without restoring the LDAP setup, or the other way round.

Instructions are included in the *Installation and Configuration Guide* and in the *User Guide for Administrators*.

2.10 Changes to requirements

An LDAP server for authentication of users is no longer mandatory. You can choose to have only local users, only LDAP users, or both.

We recommend that you have at least one local administrator account. This is to make sure that you can still access Meeting Management if there are issues with your LDAP setup. For general use in production we recommend that users are authenticated via LDAP.

We have added the following caution about TMS performance:

CAUTION: When Meeting Management is integrated with TMS and you have many scheduled meetings, you may experience performance issues with TMS. For instance, notification emails could be delayed, or meetings would start slightly late. The impact depends on how many meetings you schedule per week, as well as sizing of your TMS and its SQL database servers.

For all requirements and prerequisites for Meeting Management 2.5, see the *Installation and Configuration Guide*.

3 Resolved Issues

3.1 Resolved in 2.5.1 (build 2.5.1.65)

Reference	Issue
CSCvn94919	When using a TMS version 15.8 or greater for scheduling information with a Cisco Meeting Management version 2.5.0, no scheduled meeting information will be available. Specifically: • Upcoming scheduled meetings will not be visible on the Cisco Meeting Management interface. • Ongoing scheduled meetings will appear as unscheduled meetings on the Cisco Meeting Management interface. • There will be errors in the Cisco Meeting Management logs every five minutes due to invalid API calls to the TMS.

3.2 Resolved in 2.5.0 (build 2.5.0.59)

Reference	Issue
CSCvm10694	An LDAP group that has < or > in the path cannot be added to Meeting Management.

4 Open issues

The following are known issues in this release. If you require more details on any of these please contact

Reference	Issue
CSCvn47608	The Meeting Management Guest Operating System will incorrectly be reported as running “Other 3.x Linux (64-bit)”. Meeting Management is using an up to date version of Linux. This issue is cosmetic only and does not impact meeting operations.

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: The following TMS issues are affecting behavior seen in Meeting Management:

- CSCvm10694: If Meeting Management is restarted at a time when a scheduled meeting is running past the original end time, the meeting will appear in Meeting Management as unscheduled.
- CSCvk13742: Scheduled meetings with duration greater than 24 h will not be shown 24 h in advance as expected.

5 Interoperability

The interoperability test results for this product are posted to https://tp-tools-web01.cisco.com/start, where you can also find interoperability test results for Meeting Server.

5.1 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?

Document Revision History

Date	Description
2018-12-10	Original document published.
2018-01-15	Maintenance release

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.

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 following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

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.

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)