Cisco Meeting Management

Cisco Meeting Management 3.3

(Build 3.3.0.15)

Release Notes

August 24, 2021

Contents

Document Revision History

Table 1: Document revision history

Date	Description
2021-08-24	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.

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_3_0.zip`
- Name of upgrade image: `Cisco_Meeting_Management_3_3_0.img`
- MD5 checksum for upgrade image: `180153b2add322c42e8fedfd3952cdf8`
- SHA256 checksum for upgrade image:
  `309ba089ff64fea965b18324ad843205d5098e732e2d0a077deafdf622a7331a`
- SHA512 checksum for upgrade image:
  `8074ef09e57a461247eca819fbd17cd36364420ff2b577e02487c3506528011af8779723a`
  `8ddccae169443e780e87d2f4ca68118d88546bdb1a5ee9e6c205c60`

OVA for new installation on vSphere 6.0 or below:

- File name: `Cisco_Meeting_Management_3_3_0_vSphere-6_0.ova`
- MD5 checksum for image: `e4798cd1b745cafcf96c4c6b06ae8fea`
- SHA256 checksum for image:
  `425ec5c9b0add5f0089ae0a9f01c3b05f950b8edec9125a9e1ac837e0a3c2652`
- SHA512 checksum for image:
  `bd087aef3410358f19ed52fb878ee8365c7f69b97d0854607d8ffa7f70d8c9b302714ca0b`
  `8e47bc3734be8741afb424abd3da81596d596b7b4fc47db315a7e49`

OVA for new installation on vSphere 6.5 or later:

- File name: `Cisco_Meeting_Management_3_3_0_vSphere-6_5.ova`
- MD5 checksum for image: `3923ce531a0e64f415ff02723835b668`
- SHA256 checksum for image:
  `15963d443d425edd8d5fb7f36dd1cbe0d73905a7f85ffeb41c441987765e8b87`
- SHA512 checksum for image:
  `b183491fd1f6b1114a35270f80e041f7b79151b35fbe83d4f2f6d38031c0f22d2dba09b3b`
  `d4e66d2e95ecc50ec67fe4d1ebac9e77bec711a02462c4496bdb841`

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 announced 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.

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 3.3.

## 2.1 Integration of Cisco Meeting Server Installation Assistant with Meeting Management

From the 3.3 release onwards, the Cisco Meeting Server Installation Assistant is no longer a standalone tool, it is integrated with Meeting Management and assists in installing a simple Cisco Meeting Server instance. The prior versions of Meeting Management allowed you to add existing Meeting Servers using the Add Call Bridge option. Now, with the integration of Installation Assistant into Meeting Management, you can also configure and add a new Meeting Server. The Meeting Server that you are adding must be a Meeting Server 1000 or Virtual Machine instance with software version 3.3. Installation Assistant is not compatible for use with Meeting Server 2000.

In the Meeting Management **Server** page, the **Add Call Bridge** button is now changed to **Add Meeting Server**. Clicking the button gives you the following options:

- **Add an existing Meeting Server**: As in previous releases, you can add an existing Meeting Server by selecting this option.

- **Configure and add a new Meeting Server**: On selecting this option, Installation Assistant wizard opens and you are prompted to enter **Port** number, **Username** and **Password**. On clicking **Connect**, the deployment types are displayed.

Installation Assistant supports configuring the following Meeting Server deployments:

- SIP Bridge LDAP Import Join via Web for Guests and Users

- SIP Bridge LDAP Import

- SIP Bridge Guest join via Web

- SIP Bridge Only
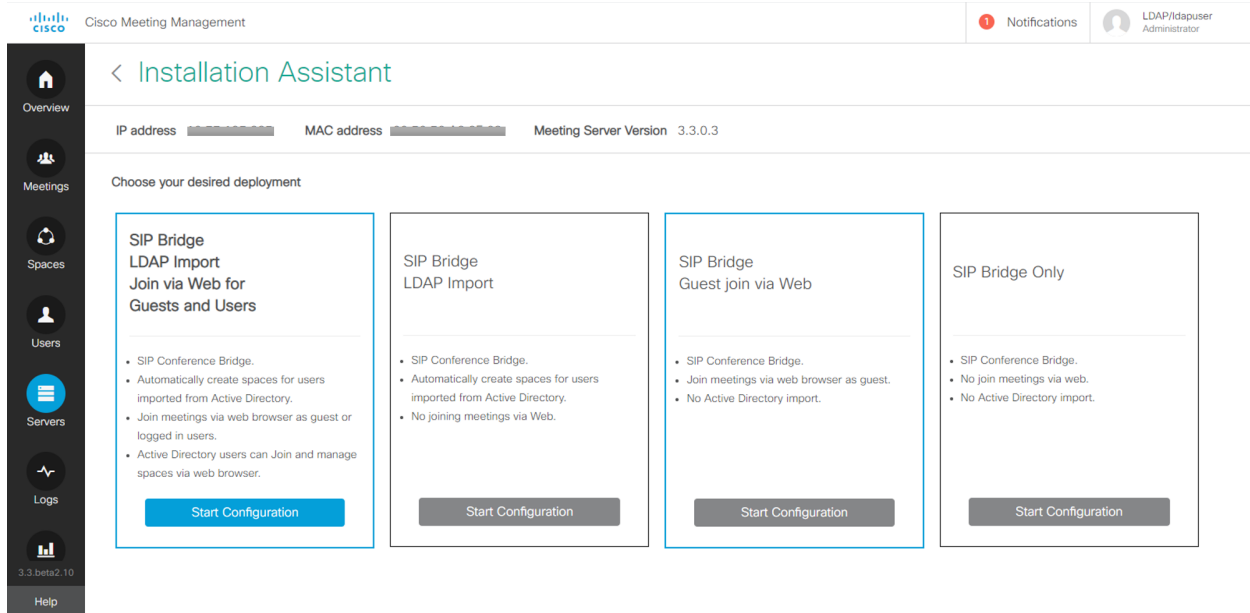
Depending on the selected deployment, the wizard navigates through all or some of the following panels that are necessary for the configuration:

- Certificate
- Network
- Call Bridge
- Web Bridge
- Conferencing User
- Security
- Push Configuration

Once the Push Configuration process is complete, the wizard displays a message about the success or failure of the configuration. If the configuration was unsuccessful or incomplete, you can do one of the following:

1. Logs: You can navigate to **Logs** tab and use **Download log bundle** button to download Meeting Management logs, which will also include the Installation Assistant logs.

2. Reset: You can use this link to remove the Meeting Server configuration pushed by the Installation Assistant.

3. Resume: You can resume configuring a Meeting Server from **Partial Configured Meeting Server** tab.

For more information on any of the above, see Cisco Meeting Management Installation and Configuration Guide.

In the **Server** page, the Meeting Server configurations are listed in the following tabs:

- **Successful Configured Meeting Server**: Successfully added Meeting Servers and their status is available in a list format. You can edit or delete the added Meeting Servers by clicking the respective icons.

- **Partial Configured Meeting Server**: Failed or pending/ incomplete configurations are listed in this tab. You can choose one of the following actions:

    a. Delete: It allows you to delete any failed or pending Meeting Server configuration.

    b. Resume: If the configuration of any Meeting Server is pending, this option allows you to resume configuration from the last unsuccessful step.

For more information see Cisco Meeting ManagementInstallation and Configuration Guide

2.2   Align web app and SIP layouts

From release 3.3 onwards, assigning layouts or pane placement from Meeting Management is supported for web app participants.

Note: Changing layouts for a single participant is not supported for web app participants.

2.3   Select default role in coSpace template creation

In Meeting Management 3.3, this feature allows administrators to select a default role for dial out participants during the meeting, while creating or editing a space template. When a participant is dialed out from the space, they join the meeting with the default role that is selected for the template. Administrator can make a role as default for dial out from a list of roles that are available for the space template using the new option **Default for dial out** available in the Meeting Management.

2.4   Admit specific participants from the Lobby

In version 3.3, video operators can admit individual participants from the lobby into an ongoing meeting. The **Lobby** pop-up screen now has a check button against each participant waiting in the lobby. Clicking on the associated button for a participant admits that participant into the meeting.

2.5   Visibility Scope

In version 3.3, the administrator can configure the Visibility Scope for an access method during template creation. When a new template is created or an existing template is edited, while adding a role, the administrator will also have the option to select a visibility scope for the template.

The visibility scope options are:

- Directory: In public directory, visible to all space members and call participants.

- Public: Visible to all space members and call participants

- Members: Visible only to space members

- Private: Visible only to the space owner (default)

For a description of how this feature works on web app, see the section *Change space member access methods* in [Cisco Meeting Server web app User Guide](#).

2.6 Changes to requirements

Meeting Management 3.3 is only supported with Meeting Server 3.3. We have updated the Hypervisor requirements for the Meeting Management VM.

For all requirements and prerequisites for Meeting Management3.3, 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 `3.3`.

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 3.3 (Build 3.3.0.15)

Reference	Issue
CSCvx11869	Users imported via Provisioning cannot log into web app via SSO.
CSCvw95093	After a meeting has ended and user closes the tab, events subscriptions kept open.

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
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)