Cisco Meeting Management

Cisco Meeting Management 3.4
(Build 3.4.0.26)

Release Notes

December 15, 2021

Cisco Systems, Inc. www.cisco.com

Contents

Document Revision History

Table 1: Document revision history

Date	Description
2021-12-15	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.
- 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 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_4_0.zip`
- Name of upgrade image: `Cisco_Meeting_Management_3_4_0.img`
- MD5 checksum for upgrade image: `87245318a0d68cfd97a5a931e4dd12e3`
- SHA256 checksum for upgrade image: `70b474952a170b781e790d14b3a57772c47538277f64f5a89c77e11da9300c5c`
- SHA512 checksum for upgrade image: `0bf0ac658357b418a5798c3becedaa8bad1df63f0b264d4c1559e2c9ebfa4d146ad3c1378a10e3255fa39e5fc4788e122b6582e648023b5248cb88c2b41f26b1`

OVA for new installation on vSphere 6.0 or below:

- File name: `Cisco_Meeting_Management_3_4_0_vSphere-6_0.ova`
- MD5 checksum for image: `2c05a8e0a9de11e41499e891af4b5003`
- SHA256 checksum for image: `f82cd19b7754464c6ad9abb2b3ddf2dfc47f80f3f09fb4bb3de2bd081a9e5159`
- SHA512 checksum for image: `c14ab3fd0f14cc4db0e2fbfe8835442849ace16a6cd7f4ca4ce9bf43afb5edf431416d43b4717ce789c6c4d5a4fc1f29ad3d03bfa5b12a023da149acfa24e8df`

OVA for new installation on vSphere 6.5 or later:

- File name: `Cisco_Meeting_Management_3_4_0_vSphere-6_5.ova`
- MD5 checksum for image: `397cb5da20612f9cac6434bdf7db2a37`
- SHA256 checksum for image: `a48102bd1304819b8ad3393244547bbbcc737978cc3439130b2f72bc8a0e2741`
- SHA512 checksum for image: `0e14351bf562e4cbe8871f43d8f9806fcac2d6b23b5b3aae02b3d286f4cdcd216c804254d38045fc70389e0d35335fee09b201c651cc92882686fa5681cc5fa8`

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 3.4 .

2.1 Removal of traditional licensing support

From 3.4 release, Meeting Management has deprecated the support for local license files (traditional licensing mode). Smart licensing is a requirement for Meeting Server from version 3.4 onwards. If you were using traditional Product Activation Key (PAK) licenses in previous versions, you must migrate to Smart Licensing and use Cisco Smart Software Manager (CSSM) for licensing.

To register with CSSM, you must have a Smart Account for your company with a dedicated Virtual Account that will be used by only one instance of Meeting Management. To request an account, talk to your Cisco account team or go to Cisco Software Central.

The **License status** in **Overview** page in Meeting Management now displays a warning for traditional licensing users, with a message to set up Smart Licensing using CSSM. In the **Licensing Mode** pop-up, Smart Licensing and No Licensing are available options to choose from.

- Smart Licensing: You must use Cisco Smart Software Manager for licensing. Your license status may show as out of compliance until you register with the Cisco Smart Software Manager and set your license allocations.
- No Licensing: This instance can only be used for managing your meetings. This instance of Meeting Management will not be listed in **Product Instances** page of Cisco SSM.

The Traditional Licensing option is grayed out for users who were using this licensing mode in previous releases. **Traditional Licensing** option is no longer available with Meeting Server and Meeting Management 3.4 version or higher.

2.2 License Reservation

To be compliant with SMART, Cisco product users require support for License Reservation. Meeting Management supports license reservation from version 3.4 onwards. In an environment where Meeting Management cannot connect to the Internet due to security reasons, License reservation can be used to activate features and reserve licenses.

The feature has two variants: Universal (Permanent License Reservation) and Specific (Specific License Reservation).

- **Universal variant**: Universal or Permanent License Reservation (PLR) provides a single license that enables use of all features in the product. PLR is meant for restricted use and is only available for Military/Defense customers.

  Contact your Cisco Account team to enable your Smart Account for PLR.
- **Specific variant**: Specific License Reservation (SLR) provides you with a choice to reserve licenses based on your requirement. In addition to feature licenses, user licenses such as SMP Plus and PMP Plus can also be reserved. If license usage changes, this feature allows updating or changing the license reservation.

  For most customers who cannot connect from Smart Licensing Manager On-Prem/Satellite to Cisco for licensing usage, SLR mode can be utilized and is available by default.

Note: You must have a Smart Account for your company with a dedicated Virtual Account that will be used by only one instance of Meeting Management.

PLR for Meeting Server or Meeting Management must be specifically ordered by the customer and approved by Cisco. To request for an account or to enable PLR on your Smart Account, talk to your Cisco account team or go to Cisco Software Central.

License reservation can be changed from Universal to Specific variant and vice versa. This involves returning the reservation and re-registering the product instance.

License reservation allows the following workflows:

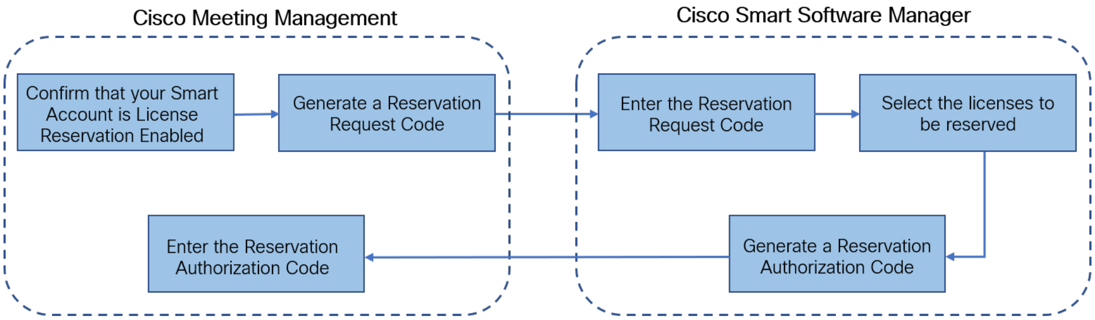
- Reserve SLR/PLR licenses
- Update reserved licenses
- Return reserved licenses

2.2.1 License Reservation

The workflow for initial license reservation is as follows:

1. Confirm that the Smart Account is License Reservation enabled
2. Generate a Reservation request code from Meeting Management
3. Enter the code in CSSM
4. In case of SLR, select license to be reserved
5. Generate a Reservation Authorization Code in CSSM
6. Enter the authorization code in Meeting Management

Figure 1: Workflow for License Reservation

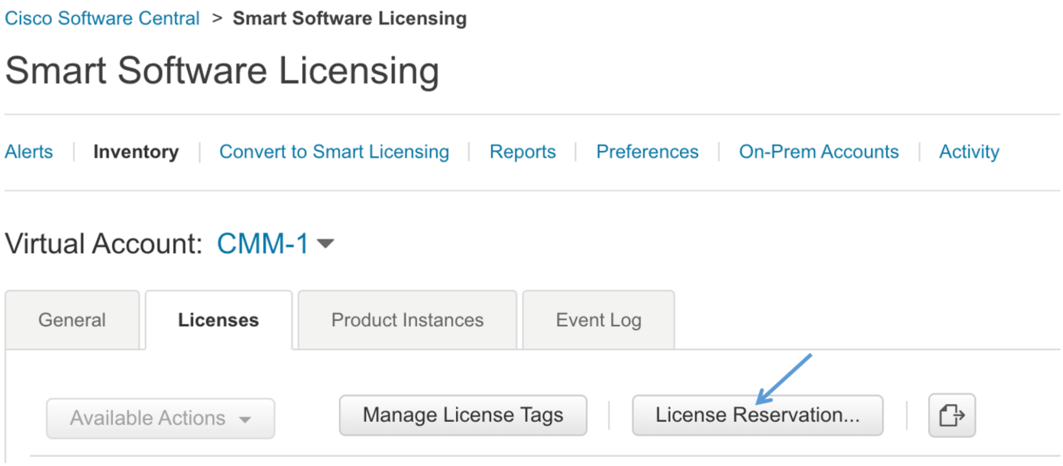

Cisco Meeting Management
Cisco Smart Software Manager
Confirm that your Smart Account is License Reservation Enabled
Generate a Reservation Request Code
Enter the Reservation Request Code
Select the licenses to be reserved
Generate a Reservation Authorization Code
Enter the Reservation Authorization Code

Follow these steps for license reservation:

1. In Meeting Management **Settings**, go to the **Licensing** section:
   a. Click the **Register** button to open **Smart Software Licensing Registration** pop-up.
   b. Click the **start here** link at the bottom of the pop-up to initiate the license reservation process.
   c. In the pop-up window that opens, click **Yes, My Smart Account is License Reservation Enabled**.
   d. In the **Smart License Reservation** pop-up, click **Generate** button to generate Reservation Request Code.
   e. Save or copy the Reservation Request Code that is generated.
   f. Click **Close**. In **Smart Software Licensing** page of Meeting Management, the **Smart Software Licensing Status** will be displayed as **License Reservation Pending**.

2. In Smart Software Manager
   a. Log in to Cisco Smart Software Licensing Manager using your Smart Account
   b. Navigate to the desired Virtual Account and click **License Reservation**

Figure 2: License reservation enabled in Smart Account


Cisco Software Central > Smart Software Licensing
Smart Software Licensing
Alerts | Inventory | Convert to Smart Licensing | Reports | Preferences | On-Prem Accounts | Activity
Virtual Account: CMM-1
General
Licenses
Product Instances
Event Log
Available Actions
Manage License Tags
License Reservation...

Note: **License Reservation** option will be visible if your Smart Account is enabled for license reservation.

   c. Enter the Reservation Request Code.
   d. Choose licensing from **Licenses to Reserve**:
      - For PLR – Select option **Meeting Server PLR Enablement**
      - For SLR – Select option **Reserve a specific license** and select the specific licenses to be reserved.
   e. Click **Generate Authorization Code** button to generate the Reservation Authorization Code.
   f. Save or copy the Reservation Authorization Code.

Note: In case of Specific licensing, on selecting **Reserve a specific license** in **Licenses to Reserve**, user can view a list of available licenses. Ensure to select enough quantity of licenses while requesting in the Smart Account.

3. In Meeting Management, perform the following steps:
    1. In **Smart Software Licensing** page, open **Enter Reservation Authorization Code** pop-up.
    2. You also have an option to view reservation request code or cancel Reservation Request
    3. Enter the Reservation Authorization Code generated from Smart Software Manager and click **Install Authorization Code/File** button to complete reservation.
4. In the **Licensing** section, the **Registration** status under **Smart Software Licensing Status** will change:
    - from **License Reservation Pending** to **Registered - License Reservation**
    - and **License authorization** as **Authorized - Reserved**.
5. The license status in the **Licenses** page will be displayed as:
    - **Reservation Active** for PLR
    - **Reserved** along with the number of licenses for SLR.

Note:
· Meeting Server APIs can also be used to fetch license status which includes, the feature components for a Meeting Server, each component's license status and expiry date. API object **`/clusterLicensing`** returns the license status and expiry date (if applicable) for a Meeting Server cluster. For more information, refer to Cisco Meeting Server API Reference Guide.
· When using Smart licensing, the MMP command **`license`** does not retrieve the license status of the virtualized server.

2.2.2 Update reserved licenses

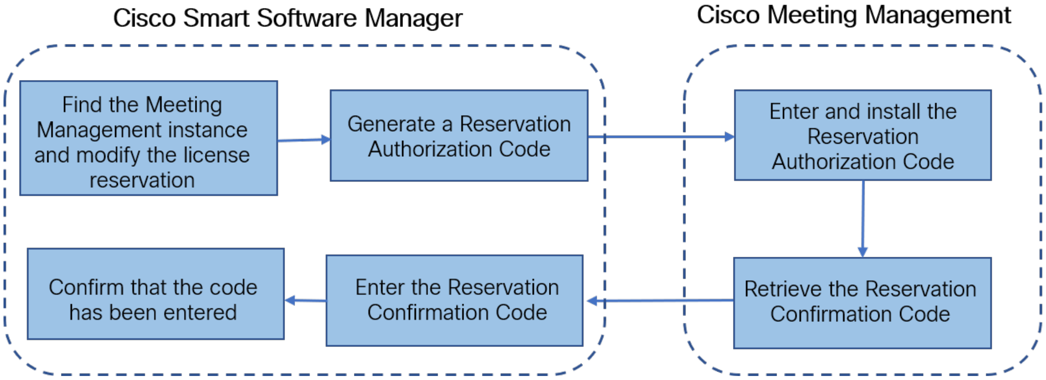
To meet the changing needs of your organization, you can update specific licenses or you can change the number of reserved licenses. For example, your current license requirement is 5 and you want to add another 5 licenses, then you need to select the number of licenses as 10 and the new value overrides the prior value.

Note: Updating licenses is not applicable in case you are using PLR. However, you can change your license reservation type from PLR to SLR or vice versa. To change the type of license reservation, return the reserved licenses, unregister the product instance, and reregister the product instance from scratch. When changing your reservation from PLR to SLR, the selected licenses in SLR will override PLR licenses.

The workflow for updating reserved license is as follows:

1. Find the license instance to be updated in CSSM
2. Generate a Reservation authorization code
3. Enter and install the code in Meeting Management
4. Generate a Reservation confirmation code
5. Enter and confirm that the Reservation confirmation code in CSSM

Figure 3: Workflow for Update License Reservation


Cisco Smart Software Manager
Cisco Meeting Management
Find the Meeting Management instance and modify the license reservation
Generate a Reservation Authorization Code
Enter and install the Reservation Authorization Code
Retrieve the Reservation Confirmation Code
Enter the Reservation Confirmation Code
Confirm that the code has been entered

Follow these steps to update the reserved licenses:

1. In Smart Software Manager:
   a. Find Cisco Meeting Management instance from the **Product Instances** and select **Update License Reservation** from the **Actions** menu.
   b. Use the **Update License Reservation** pop-up to modify the licenses to be reserved and generate a new Reservation Authorization Code.
   c. Save or copy the Reservation Authorization Code.
2. In Meeting Management **Settings**,
   a. Navigate to the **Licensing** section and click on **Update Reservation** button.
   b. Enter the Reservation Authorization Code in the pop-up that gets open on clicking **Update Reservation** button.

   Note: In case the Meeting Management instance has reserved a Universal license, to update license reservation, return this license using **Return Reserved Licenses** button in **Licensing** section and then reregister the product instance.

   c. Click **Install Authorization Code** button to update license reservation and to generate a Reservation Confirmation Code.
   d. Copy or save the Reservation Confirmation Code by clicking **View confirmation code** button in **Smart Software Licensing** page.

3. In Smart Software Manager,
    a. Find Cisco Meeting Management instance in **Product Instances** and select **Enter Confirmation Code...** from the **Actions** menu to launch the **Enter Confirmation Code** pop-up.
    b. Enter the Reservation Confirmation Code into the **Enter Confirmation Code** pop-up.
    c. Return to the **Smart Software Licensing** page in Meeting Management and click **Code Has Been Entered** button to dismiss the alert that was placed after the Reservation Authorization Code was installed.

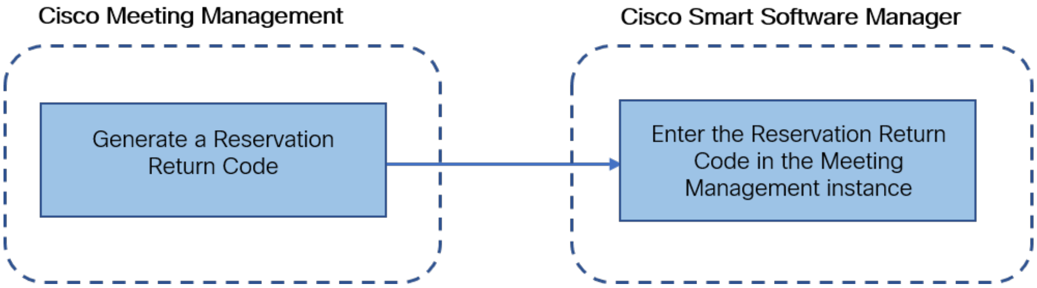
2.2.3 Returning reserved licenses

You can return the reserved licenses to the Virtual Account so that the licenses can be used by other product instances. To return licenses, follow the steps described in this section.

The workflow for returning a reserved license is as follows:

1. Generate a Reservation return code
2. Find the Meeting Management instances in CSSM
3. Enter the Reservation return code

Figure 4: Workflow for Returning License Reservation


Cisco Meeting Management
Cisco Smart Software Manager
Generate a Reservation Return Code
Enter the Reservation Return Code in the Meeting Management instance

Follow these steps to return reserved license:

1. In the **Licensing** section of Meeting Management **Settings**,
    a. Click **Return Reserved Licenses...** button to launch the **Confirm Return Licenses** pop-up.
    b. Click **Generate** button to generate a Reservation Return Code.
    c. The **License Reservation Return Code** pop-up provides instructional text and allows to copy or download a file containing the License Reservation Return Code.

2. In Smart Software Manager,
   a. Find the Meeting Management instance in **Product Instances**
   b. Select **Remove** from the **Actions** menu to launch the **Remove Product Instance** pop-up.
   c. Enter the Reservation Return Code into the pop-up to complete returning reserved licenses. The **Registration** status is changes to **Deregistered** in the **Licensing** page.

2.3 Blast Dial

In previous release, participants could join the call by pressing any key and did not have option to deny/reject the call. If the participant did not accept the call, Meeting Management continues to re-dial until it reaches the maximum number of retries as configured. This release includes an enhancement to the blast dial feature. Meeting Management now stops dialing a participant based on the DTMF key pressed by the participant. A new audio prompt guides the participants with DTMF key options to accept or reject the call. Participants can join a call only when they press the DTMF key **1**. Meeting Management stops re-dialing a participant when they press DTMF key *****. Participant can also reject a call by pressing **Decline** or **Reject** buttons.

Note: Any other DMTF inputs will be ignored and Meeting Management will continue to re-dial the participant until they press **1** or *****.

2.4 Moving participants to lobby

In this release of Meeting Management, the video operators can move specific or all participants to lobby during a meeting using the new **Move to Lobby** option. This option is enabled only if the meeting is locked.

To move a participant to lobby, select the participants in the meeting and then click **Move to Lobby**. You can also move individual participant to lobby using the lobby icon on the **Actions** tab in the participants list. Once the participant is moved to lobby, a notification is displayed indicating participants' move. To view the list of participants who are moved to lobby, click on the **Lobby** link available in the meeting information.

If the Meeting Server administrator has allowed a participant to directly enter a locked meeting without waiting in the lobby, the video operator cannot move such participants to lobby.

2.5 Change User Role

Web app allows users to change the role of other participants in the meeting. This was only supported using the Cisco Meeting Server APIs. From version 3.4, Meeting Management administrators can create or edit access methods to permit the participants to change the role of other participants in a web app meeting. This is enabled by the **Change user role** option.

While provisioning a role, you can select **Change user role** to permit the user to change the role of other participants in a web app meeting. By default participants will not have permission to change the role of other participants. For more details on provisioning a role refer to the sections Provisioning - Allow users to create spaces and Provisioning - Automatically create spaces in Cisco Meeting Management User Guide for Administrators.

2.6 Add Meeting Server Edge nodes

From version 3.4, Meeting Management allows you to add configured Meeting Server Edge nodes along with the Call Bridges. The configured Edge nodes can be added using the **Add Servers** option on the **Servers** page.

On the **Servers** page, the **Add Meeting Server** button is now changed to **Add Server**. Clicking this button gives you the following options:

- **Add Configured Server**: From 3.4 administrators can add Call Bridge and Edge nodes. To add a configured Call Bridge or an Edge node, configure the Server address, Port, Display name, Username and Password.
- **Configure New 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. You can then select the deployment type and proceed with Meeting Server configuration.

On the **Servers** page, successfully added Call Bridges and Edge nodes and their status are listed in **Configured Server** tab. Failed or incomplete Meeting Server configurations are listed in **Partial Configured Server** tab.

Refer to Cisco Meeting Management User Guide for Administrators for more details.

2.7 Run SSH commands on the Meeting Server

SSH capability is required to perform tasks on the Edge nodes added on Meeting Management. Administrators can now connect to the SSH terminal and run MMP commands on the selected Meeting Server or Edge nodes. The **SSH terminal** tab is added on the **Servers** page. You can select a Call Bridge or an Edge node and connect to the SSH terminal by providing the MMP user credentials. Once connected you can run MMP commands on the selected server.

2.8 Meeting Server logs

Version 3.4 introduces enhancements to Cisco Meeting Management logs feature. In previous releases, you could download log bundle, configure system log servers and audit log servers for tracking activity, download crash reports, and trace detailed log for only Meeting Management. From this release, Meeting Management administrators can download log bundle and trace detailed logs for Meeting Server and Edge nodes using the new tab **CMS logs**, added on the **Logs** page.

2.8.1 Meeting Server detailed tracing

Meeting Management allows the administrators to trace logs of different Meeting Server modules like SIP, Active Control, Active Speaker, ICE and so on. Administrator can click **Select Server** button and select Call Bridges from a list of servers to trace the detailed logs.

Note: To generate log bundle for all the nodes in a cluster, on the **Select Server** page while selecting the cluster node, ensure that you select each node in the cluster.

In the **Traces** list, you can enable or disable tracing for different Meeting Server components. To disable detailed tracing for all Meeting Server components, click **Disable all**. You can also set how often you want to trace the logs. For example, you can configure to trace logs for every 10 or 60 minutes or you can set an interval of your choice in the **hh:mm** format.

Note: Enabling tracing debug is an overload on the selected servers. Ensure that you enable detailed tracing only when necessary.

For more details on Meeting Server detailed tracing, see Cisco Meeting Management User Guide for Administrators.

2.8.2 Meeting Server log bundle

Meeting Management allows administrators to collect the logs for servers including Call Bridge and Edge nodes after adding them. Administrator can click **Select server** button and select Call Bridge or Edge nodes from a list of servers and click **Generate log bundle** button to generate the log bundle.

Note: To generate log bundle for all the nodes in a cluster, on the **Select Server** page while selecting the cluster node, ensure that you select each node in the cluster.

After the log bundle is generated, you are given an option to download the logs of the selected server. The generated log bundle is named **logbundle_<host name>_YYYY-MM-hh-mm-ss.tar.gz**. The generated logs can be downloaded within 24 hours from the **CMS log bundle** page.

For more details on generating and downloading the log bundle, see Cisco Meeting Management User Guide for Administrators.

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 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
CSCvz89972	In a locked meeting, Meeting Server administrator can provide permission to participants to enter the meeting, without waiting in the lobby. When the video operator moves such participants to lobby a success message **Participant has been moved to lobby successfully** is displayed even if the participant was not moved to the lobby.
CSCwa36281	After restoring Meeting Management from a backup, when license mode is changed from **No licensing** to **Smart licensing**, administrator is unable to view Smart licensing screen and an error message **Could not fetch licenses please refresh** is displayed. When taking the backup, license mode was selected as **Smart licensing** and license status was **deregistered**. This issue is resolved when the administrator upgrades Meeting Management with the same build.
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.

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: 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."

5 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.

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?

6 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

6.1 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