Cisco Meeting Management

Release 4.0

(Build 4.0.0.22)

Release Notes

November 11, 2026

Contents

Document Revision History 1

1 Introduction 1
1.1 The software 1

2 New features and changes 2
2.1 Email Alerts for License Utilization 2
2.2 Encryption Licensing for Meeting Server 4
2.3 Optimized custom layout performance 5
2.4 Deploying Meeting Management using NFVIS 6
2.4.1 Deployment Workflow Summary 6

3 Upgrading, downgrading and deploying Cisco Meeting Management 7
3.1 Upgrading from previous version 7
3.2 Downgrading to previous version 8
3.3 Deployments 9
3.3.1 VMware ESXi Deployment 9
3.3.2 Nutanix Deployment 9
3.3.3 NFVIS Deployment 9
3.4 Checksums for upgrade and installation files 9
3.5 Smart Licensing 10
3.6 End of software maintenance for earlier versions 11
3.6.1 End of software maintenance 11
3.6.2 Discontinuation of CMM integration with Telepresence Management Suite 11
3.7 Meeting Management and connected Meeting Servers must run the same software version 11

3 Bug search tool and resolved and open issues 12
3.8 Using the bug search tool 12
3.9 Open issues 12
3.10 Resolved Issues 14

4 Interoperability 16
4.1 Mute/unmute and layout behaviors 16

5 Product documentation 17
5.1 Related documentation 17

Accessibility Notice 18

6 Accessibility support features 19

6.1 Keyboard navigation 19

6.2 Screen reader support 19

Cisco Legal Information 20

Cisco Trademark 21

Document Revision History

Table 1: Document revision history

Date	Description
Nov 11, 2026	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.

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.

2 New features and changes

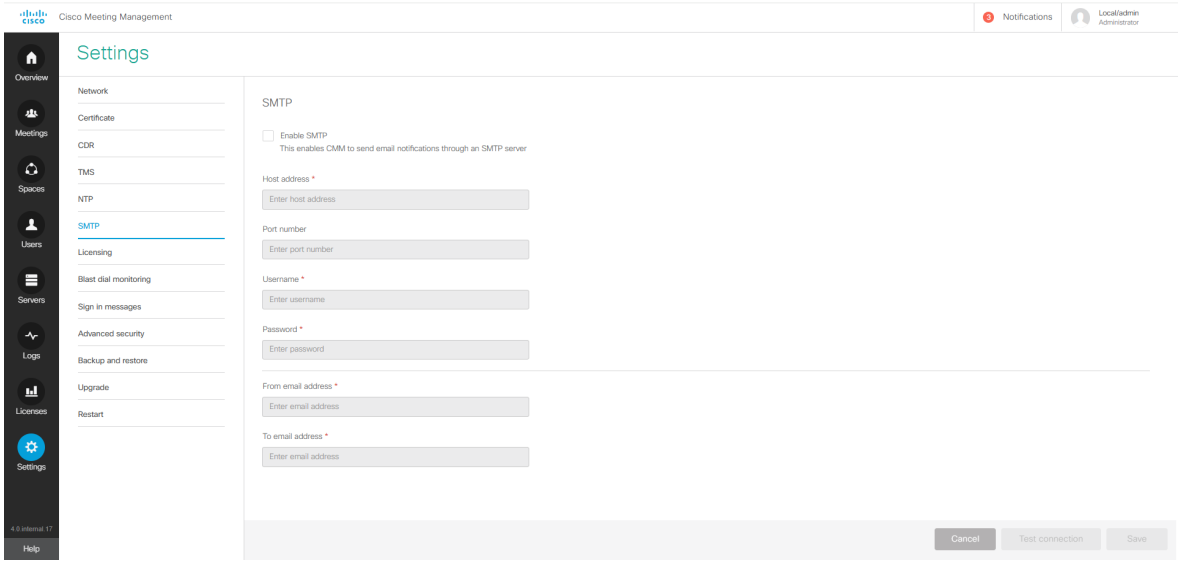
In this section you can see what is new in 4.0.

2.1 Email Alerts for License Utilization

From version 4.0,Meeting Management supports automated email notifications for licensing compliance. Administrators can configure an email address to receive alerts when license usage limit exceeds or when the system falls out of licensing compliance. This provides timely visibility, helps prevent unintended enforcement, and reduces the need for frequent manual dashboard checks.

A new **SMTP** page has been added to the **Settings** tab. Enabling the **Enable SMTP** checkbox allows the administrator to configure an SMTP server to send email notifications. To configure an outbound SMTP server, follow these steps:

1. Enter the address of SMTP server in **Host address**.
2. Enter the port number used by SMTP server in **Port number**.
3. Enter the credentials required for SMTP authentication in **Username** and **Password**.
4. Enter the email address that will appear as the sender for notifications in **From Email address**.
5. Enter the destination email address where notifications will be sent in **To Email address**.



6. Click the **Cancel** button to reset the details you have entered.

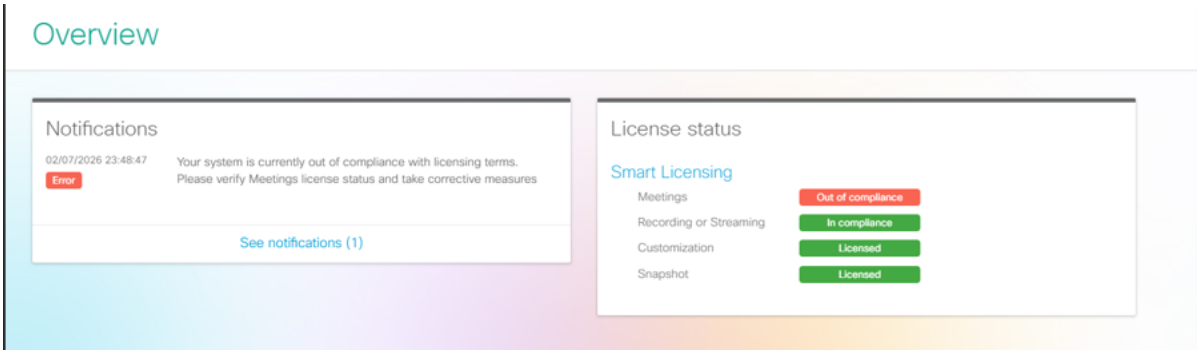
7. Click **Test connection** to verify the server connection. A successful connection triggers a verification email, confirming the "From" address is authorized to send and the "To" address can receive email notifications.
8. Once connected, click the **Save** button to apply your changes. Note that a system restart is required to activate licensing compliance notifications.

Meeting Management 4.0 utilizes standard SMTP only for license-alert notifications; SMTPS (implicit SSL) and STARTTLS are not supported. If credentials are provided, Meeting Management attempts to authenticate using AUTH LOGIN during the initial unencrypted SMTP session. Consequently, the mail server must advertise LOGIN or PLAIN mechanisms in its unencrypted EHLO response. "Test connection" will fail if the server only advertises NTLM or requires STARTTLS before offering LOGIN. When authenticating, the "From" address must be an identity the account is authorized to use (e.g., the mailbox itself, an alias, or a delegated "Send As" address). Note that "Test connection" results are displayed only in the UI and are not recorded in the Meeting Management system logs.

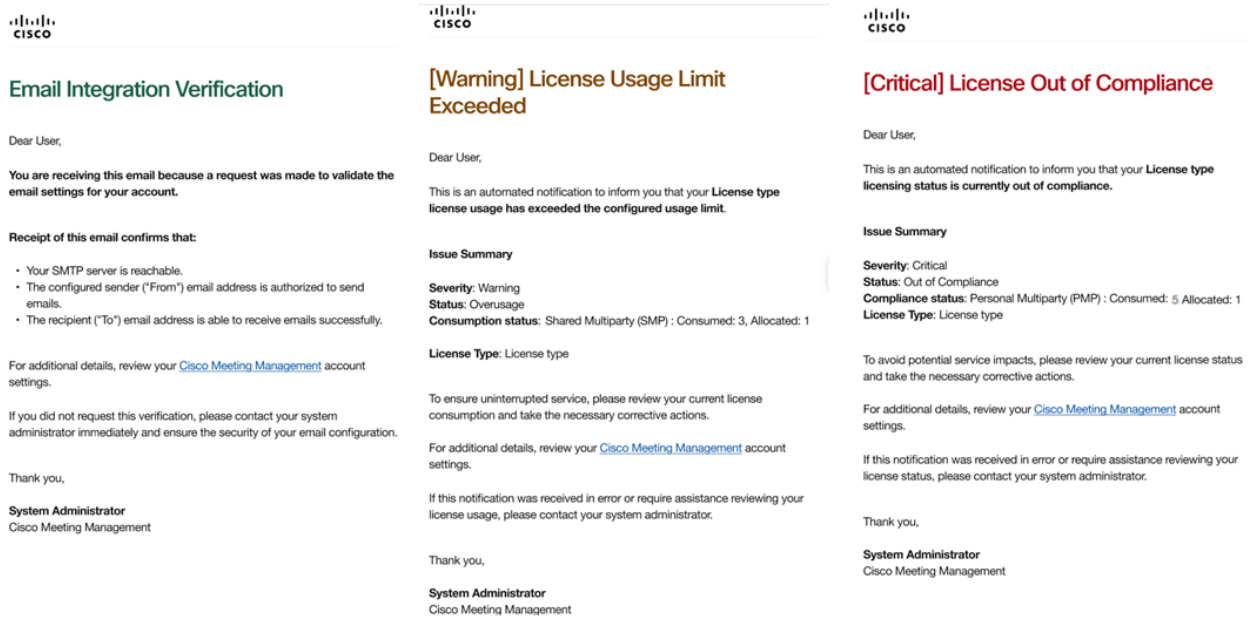
Note:

- SMTP username and password are mandatory fields. Anonymous configurations are no longer supported.
- Meeting Management provides specific error messages for host connection, authentication, and email delivery failures to assist in troubleshooting.
- A successful connection is confirmed only upon receipt of the verification email.

When the licenses are out of limit/out of compliance alerts linked to license usage available in the **Notifications** section of the Meeting Management **Overview** page are sent as email notifications.



The system sends the following email notifications based on the license usage type.



Email Integration Verification

Dear User,

You are receiving this email because a request was made to validate the email settings for your account.

Receipt of this email confirms that:

- Your SMTP server is reachable.
- The configured sender ("From") email address is authorized to send emails.
- The recipient ("To") email address is able to receive emails successfully.

For additional details, review your Cisco Meeting Management account settings.

If you did not request this verification, please contact your system administrator immediately and ensure the security of your email configuration.

Thank you,

System Administrator
Cisco Meeting Management

[Warning] License Usage Limit Exceeded

Dear User,

This is an automated notification to inform you that your **License type license usage has exceeded the configured usage limit**.

Issue Summary

Severity: Warning
Status: Overusage
Consumption status: Shared Multiparty (SMP) : Consumed: 3, Allocated: 1

License Type: License type

To ensure uninterrupted service, please review your current license consumption and take the necessary corrective actions.

For additional details, review your Cisco Meeting Management account settings.

If this notification was received in error or require assistance reviewing your license usage, please contact your system administrator.

Thank you,

System Administrator
Cisco Meeting Management

[Critical] License Out of Compliance

Dear User,

This is an automated notification to inform you that your **License type licensing status is currently out of compliance.**

Issue Summary

Severity: Critical
Status: Out of Compliance
Compliance status: Personal Multiparty (PMP) : Consumed: 5 Allocated: 1
License Type: License type

To avoid potential service impacts, please review your current license status and take the necessary corrective actions.

For additional details, review your Cisco Meeting Management account settings.

If this notification was received in error or require assistance reviewing your license status, please contact your system administrator.

Thank you,

System Administrator
Cisco Meeting Management

The email notifications will be triggered once in case:

- Meeting license usage has reached the limit, resulting in insufficient licenses
- Meeting license is out of compliance
- Recording/Streaming license usage has reached the limit, resulting in insufficient licenses
- Recording/Streaming license is out of compliance
- SMTP server is configured to send verification email to validate email integration.

Note: The system classifies license status based on the following criteria:

- Insufficient License: Usage exceeds capacity for 1–14 days in a 90-day window.
- Out of Compliance: Usage exceeds capacity for 15+ days in a 90-day window.

2.2 Encryption Licensing for Meeting Server

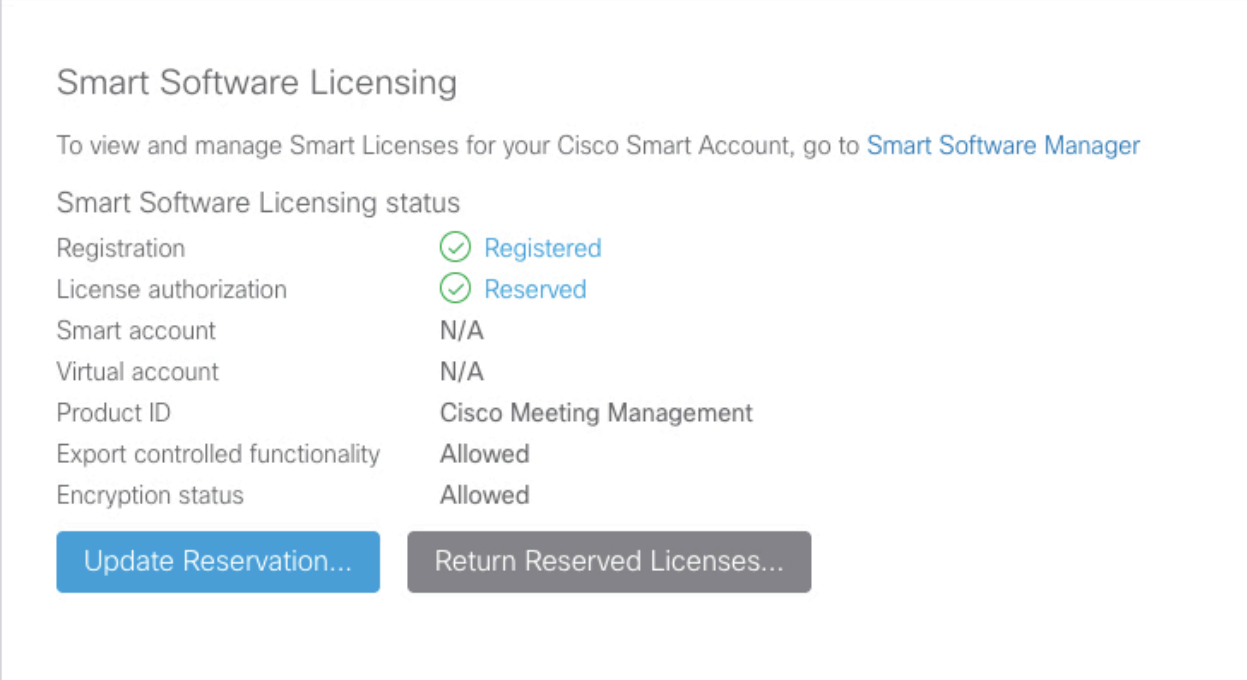
In version 3.11, Meeting Management introduced the encryption license for customers in category C and D countries to enable call encryption. Starting with version 4.0, this license is now recommended for all customers to enable encryption on Meeting Server call bridges.

The following table outlines how Meeting Management validates the LIC-CMS-ENCRYPT-S license in Smart Account:

Table 2: Meeting Management validation of LIC-CMS-ENCRYPT-S license in Smart Account

Call Encryption Status	Actions performed by Meeting Management	License reservation and encryption
Encryption license (LIC-CMS-ENCRYPT-S) is available	Allows encryption	License reserved and enabled encryption.
Encryption license (LIC-CMS-ENCRYPT-S) is not available	If Export control is allowed	If allowed: Allows encryption only for Smart accounts in category A or B
Encryption license (LIC-CMS-ENCRYPT-S) is not available	If Export control is not allowed	Do not allow encryption for Smart accounts in category C or D

Administrators can view current encryption status in Meeting Management in the new **Encryption Status** field added in the **Licensing** page in **Settings** tab.



Note: Encryption licenses are required per deployment; ensure that sufficient licenses are purchased to cover all the Meeting Management instances.

2.3 Optimized custom layout performance

From version 4.0, Meeting Management improves video layout responsiveness while applying pane placement by reducing the custom layout latency. Custom layouts now apply with the same speed and consistency as standard layouts. This ensures a faster, more consistent experience for administrators and video operators while applying pane placements during live meetings.

2.4 Deploying Meeting Management using NFVIS

From version 4.0, Network Function Virtualization Infrastructure Software (NFVIS) serves as the virtualization foundation for Meeting Management, providing a streamlined, robust infrastructure to host and manage the virtual instances required for meeting environment.

2.4.1 Deployment Workflow Summary

1. **CIMC Initialization**: Access the Cisco Integrated Management Controller (CIMC) management port to verify hardware health (Power: ON, Status: Good) and configure the management network via the F8 utility if not pre-configured.
2. **NFVIS Installation**: Mount the NFVIS ISO via the CIMC Virtual Media menu. Boot the server using the Cisco vKVM-Mapped vDVD option and follow the installer prompts to deploy the OS to the target disk.
3. **Network Configuration**: Once installed, access the NFVIS CLI to assign the management IP and LAN bridge interface. Ensure the correct port (e.g., GE15-0) is assigned to the LAN bridge and disable DHCP on the WAN bridge to prevent network conflicts.
4. **Gateway & Verification**: Define the default gateway and perform a final connectivity matrix check (ping gateway/external, verify SSH access, and confirm Web UI accessibility) to ensure the system is ready for production.

To deploy a VM on NFV Infrastructure Software:

1. Log in to the NFVIS portal.
2. Upload the VM image under **Configuration** → **Image Repository**; set **VM Workload Type** to **Calling** → **CMM** and wait for the image to become **ACTIVE**.
3. Deploy the VM via **Configuration** → **Deploy** by selecting **Calling** → **CMM**, filling in details, and clicking **DEPLOY**.
4. Verify the VM status is **Active** under **Configuration** → **Manage** → **Virtual Machine**.
5. Edit the VM to assign **nic0** to the **lan-net** network and submit.
6. Access the VM console from the **Manage Deployments** page for setup and troubleshooting.

For complete steps for deploying Meeting Management in NFVIS, refer to **Deployments** section in Cisco Meeting Management Installation Guide.

3 Upgrading, downgrading and deploying Cisco Meeting Management

3.1 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.

Upload keys to verify upgrade images:

Cisco Meeting Management embeds a signature within the upgrade image to confirm whether or not the image is genuine.

Image signatures are automatically verified when upgrading from a signed image. Manual verification of hashes is still advised when upgrading from an unsigned image to a signed one, or when downgrading to earlier versions. This feature is fully effective for upgrades from version 3.7.

When upgrading to a special build, administrators must upload a special key. The **Upload Key** button is provided to allow administrators to upload the public key and verify these images. However, this action is only required when performing an upgrade to a special build.

To upload public keys:

1. On the **Settings** page, go to **Upgrade** tab.
2. Click **Upload key** then browse and select the public key. The selected public key is verified and uploaded.

Note: Upgrades from a signed production/ special build to another signed production build will not require any action from the administrator. Meeting management verifies the upgrade images automatically without the need for manual verification of the hashes.

Note:

- Prior to upgrading to version 4.0, ensure that a fully qualified domain name (FQDN) is configured in the network settings. Using an incomplete hostname may result in login failures.
- If the hostname in Network settings is not set to an FQDN before upgrading, Meeting Management can still be accessed via its IPv4 address, and the hostname can be updated to the FQDN afterward.

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.

3.2 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** in Cisco Meeting Management Administrator's Guide

3.3 Deployments

From version 4.0, Meeting Management supports deployments on VMware, Nutanix and NFVIS clusters.

3.3.1 VMware ESXi Deployment

When uploading OVA to vCenter and deploying, the Publisher field should show (Trusted certificate). If you see a warning for an invalid certificate and not-trusted cert when importing the OVA, see this article: https://kb.vmware.com/s/article/84240. You may have to add the intermediate and root certificates corresponding to the certificate used to sign the OVA, to the VECS Store. To procure intermediate or root certificates or any other issues, contact Cisco Technical Support.

Note: This release of version 4.0 supports ESXi 8.0 U3k

3.3.2 Nutanix Deployment

Version 4.0 of Meeting Management supports deployment with the following specifications:

AHV: 10.3.1.2

AOS: 7.3.1.2

3.3.3 NFVIS Deployment

Version 4.0 adds support to deploy Meeting Management on NFVIS clusters with the following specification:

26.2.1-FC1

3.4 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_4_0.zip**
- Name of upgrade image: **Cisco_Meeting_Management_4_0.img**
- MD5 checksum for upgrade image: **9db5629ae3bd2e093d603f8822316fbf**
- SHA256 checksum for upgrade image: **8b1b3e55a2c543f7c673e4e064dd46f0f2f6e4c0ae080d3c35f0f03401066cbc**
- SHA512 checksum for upgrade image: **88c3eb80dcdbfadac1d49868796f8bac45c101c2c3b5d0476b2e541d0eea546b6032bff1ff609c03393ff8cc16a5c23c1b619958d4dd4c82decde3f5e6926902**

OVA for new installation on vSphere 8.0:

- File name: **Cisco_Meeting_Management_4_0.ova**
- MD5 checksum for image: **38660d19b44b5ad4a635ae9fc25764f0**
- SHA256 checksum for image: **d4a9a82a882284315eca0d091d3891b09aa4c1acb314f7a538f0b2635bd0245d**
- SHA512 checksum for image: **62691ea42186136703569a768babe315c802edc1606f9f784c3cf391b2932cacd7acdb53158460a01dc8cca40bb9da7189aa983d6f714cebac57ea69b009fa52**

Note: This release of version 4.0 supports ESXi 8.0 U3k. Nutanix specifications will be **AHV:** 10.3.1.2 and **AOS:** 7.3.1.2. NFVIS Version: 26.2.1-FC1.

3.5 Smart Licensing

Smart licensing is mandatory for Meeting Management. All web proxy configurations used for Smart Licensing must be established as an HTTPS proxy.

To maintain secure communication, the proxy must support end-to-end HTTPS connectivity between the Meeting Management client, the proxy, and the Cisco Smart Software Manager (CSSM).

Note: This requirement represents an update from previous versions (prior to 3.13), where a standard HTTPS-capable proxy was sufficient. This change has been implemented to align with updated security standards and to ensure a more robust, secure connection for your environment.

For more information on Smart Licensing and upgrading , see Cisco Meeting Management User Guide for Administrators.

3.6 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.

3.6.1 End of software maintenance

Table 3: Timeline for End of Software Maintenance for versions of Meeting Management

Cisco Meeting Management version	End of Software Maintenance notice period
Cisco Meeting Management version 3.12	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes for Cisco Meeting Management version 3.12.x is May, 2027

3.6.2 Discontinuation of CMM integration with Telepresence Management Suite

The integration of Telepresence Management Suite and Meeting Management will be discontinued in future releases due to Telepresence Management Suite approaching its end of life.

3.7 Meeting Management and connected Meeting Servers must run the same software version

Meeting Management and connected Meeting Servers must run the same software 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.

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.

3.8 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 **`3.5`**.
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.

3.9 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
CSCwr59626	During an ongoing meeting, if Meeting Management is restarted, the blue indicator does not appear when applying a template at the per-participant level, potentially causing pane placement for new participants to malfunction.
CSCwr77094	The pane placement configuration icon displays the blue indicator even after disabling pane placement for all participants using the **Select All** check box.
CSCwo81112	When the Meeting Management administrator or video operator attempts to control a SIP participant's camera via the **front-end camera control** option, the participant receives no notification while their camera is being controlled.

Reference	Issue
CSCwo81113	Creating space using Meeting Management do not include webBridgeAddresses in the **Join Link**, which is configured on the webBridgeProfiles in Meeting Server, causing an issue in joining this space via the web app.
CSCwo81114	When a guest participant is moved from one meeting to another meeting, the Device IP and Device Type are being displayed as N/A in the participant info card.
CSCwo81116	When an administrator or video operator mutes a participant's audio and video in a meeting, and the participant is moved to another meeting with the **retain audio-video settings** check-box enabled, they cannot unmute their audio or video until the administrator manually re-enables them.
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.
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."

3.10 Resolved Issues

Resolved in 4.0 (Build 4.0.0.22)

Reference	Issue
CSCwv66195	Meeting Management allows video operators to bypass tag restrictions for Meetings and Participants, which allows operators to interact with resources outside their assigned tags via REST APIs, WebSockets, and camera controls.
CSCww60557	Meeting Management allows video operators to bypass tag restrictions, enabling unauthorized access to meeting data and Meeting Server backed meeting controls for spaces outside their assigned scope due to inconsistent tag validation.
CSCwv83235	Meeting Management requires non-deterministic PRNG to construct meeting URIs and call IDs for meetings.
CSCwu48279	Smart licensing registration process lacks a retry limit or backoff mechanism, causing the system to enter an infinite retry loop when encountering connection failures.
CSCwv55459	Dial Blast functionality for a coSpace may fail if the primary Meeting Server node is unreachable from Meeting Management.
CSCww60578	Meeting Server administrator credentials and space passcodes are not masked and appear in Meeting Management logs.
CSCww60562	Local user accounts with pending password changes could still maintain active connections, enabling continued unauthorized access to real-time meeting data.
CSCwv01038	Meeting Management PCAP sessions remains active after a system restart. Post restart, pcap continues to run when navigating to **Logs > PCAP**.
CSCwv66190	A vulnerability in the Meeting Management firmware upgrade process allows undetected modification of files larger than 64KB.
CSCwv01073	Meeting Management appliances disclose their internal system time by answering ICMP timestamp (Type 13) requests. This happens because default Linux kernel settings and a lack of firewall rules at boot allow these requests to be processed.

Reference	Issue
CSCwt67239	Meeting Management do not allow to configure Local user password with special character hyphen(-) in Users page when the password complexity is enforced.
CSCwv66202	Meeting Management uses random integers to construct meeting URIs and call IDs for meetings.
CSCwu86560	Sensitive passcode data of the spaces created in Meeting Management are exposed as plain text in Meeting Management logs.
CSCwv66207	Background task system of Meeting Management was configured to use Python's pickle format for task messages. This allows attackers with broker access to execute code on Meeting Managementworkers via malicious messages.
CSCwv66211	Meeting Management web application lacks HTTP Host header validation, allowing requests to any hostname and undermining verification of the intended target.
CSCwr97351	An attacker with access to the internal task broker could potentially send a crafted message that runs code in a Meeting Management worker.

4 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.

4.1 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?

5 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

5.1 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

6 Accessibility support features

6.1 Keyboard navigation

You can use your keyboard to navigate through Meeting Management.

- Use **Tab** to navigate between areas in Meeting Management. You'll know an area is in focus when it's surrounded by an outline. Use **Shift + Tab** to move to the previously focused area.
- Use the **Spacebar** or **Enter** key to select items.
- Use arrow keys to scroll through lists or drop-down menus.
- Use **Esc** to close or dismiss opened screens/menus.

6.2 Screen reader support

You can use the JAWS screen reader version 18 or later.

The screen reader announces focused areas/buttons, relevant information like notifications, warnings, status messages appearing on the screen, and the actions you can perform.

For example: When you focus on **Create Space** button, the screen reader will announce "Create Space" and to enter a space name.

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.

© 2026 Cisco Systems, Inc. All rights reserved.

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)