

# Cisco Meeting Management

Cisco Meeting Management 3.7

(Build 3.7.0.24)

Release Notes

March 16, 2023

# Contents

Document Revision History .....	3
1 Introduction .....	4
1.1 The software .....	4
1.2 Upgrading from previous version .....	4
1.3 Downgrading to previous version .....	6
1.4 Checksums for upgrade and installation files .....	6
1.5 Smart Licensing .....	6
1.6 End of software maintenance for earlier versions .....	7
1.6.1 End of software maintenance .....	7
1.7 Meeting Management and connected Meeting Servers must run the same software version .....	7
2 New features and changes .....	8
2.1 Reset Meeting Server Password .....	8
2.2 Applying pane placement in custom layouts .....	10
2.3 Image signing .....	11
2.3.1 Signed image file naming convention .....	13
2.3.2 Key file naming convention .....	14
2.3.3 File naming examples .....	14
2.4 Accessibility improvements .....	14
3 Bug search tool and resolved and open issues .....	16
3.1 Using the bug search tool .....	16
3.2 Resolved Issues .....	16
3.3 Open issues .....	17
4 Interoperability .....	19
4.1 Mute/unmute and layout behaviors .....	19
5 Product documentation .....	20
5.1 Related documentation .....	20
Accessibility Notice .....	21
Cisco Legal Information .....	22
Cisco Trademark .....	23

# Document Revision History

Table 1: Document revision history

Date	Description
2023-03-16	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.

Upload keys to verify upgrade images:

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

Image signatures are only verified when upgrading from a signed image. So manual verification is still advised when upgrading from an unsigned image to a signed one. i.e. if you upgrade from 3.6 to 3.7, or downgrade to earlier versions, you are still advised to manually verify the hashes. This feature will be fully effective when upgrading from 3.7 and beyond.

From version 3.7, upgrading to a special build will require uploading a special key. The **Upload Key** button is introduced to enable administrators to upload the public key and verify the upgrade images. However, the administrators will perform this action only when upgrading 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.

---

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_7_0.zip`
- Name of upgrade image: `Cisco_Meeting_Management_3_7_0.img`
- MD5 checksum for upgrade image: `39b95cdf8aabf5262e82ce3d002aeb30`
- SHA256 checksum for upgrade image:  
`7926aecbc1f31bc656b800f381d84d244fc90fed4016f6d7f02cddd44835061`
- SHA512 checksum for upgrade image:  
`74a269f4171248c67a9b64cbf9c396045ea02bf1786a76a066f6130ad333457b2750baa5d62e091768732d007c50c229d484a0a23e7b6e90b273e0f931072d52`

OVA for new installation on vSphere 6.5 or later:

- File name: `Cisco_Meeting_Management_3_7_0_vSphere-6_5.ova`
- MD5 checksum for image: `5597daf1f92757b152fd1ca72b6d6564`
- SHA256 checksum for image:  
`a74c68d67f9867a9d35f740815d03ef13791add644a46e1b2badd2a3fe62dc6`
- SHA512 checksum for image:  
`95c986ec2abfc7480637af2cf9b9f67f92cdf3682eb5827e19f35b002be6381e142280604c4e4ee9c441ba3e0faac5bcbd360a726ca156f5b7e05d1cc0eccf1e`

---

Note: From version 3.7, Meeting Management does not support ESXi versions 6.0 and below. The .ova files for these versions (ESXi 6.0/5.5) will not be provided. This version of Meeting Management supports ESXi versions 6.5 PO9, 6.7 PO8, 7.0 U3j.

---

### 1.5 Smart Licensing

From the 3.4 release onwards, Smart licensing is mandatory for Meeting Management. The support for traditional licensing has been deprecated from 3.4 and later releases. Customers are advised to move to Smart licensing.

For more information on Smart Licensing and upgrading, see [Cisco Meeting Management User Guide for Administrators](#).

---

Note: Cisco Smart Licensing Cloud Certificates were updated on January 15, 2023. Customers using Direct Mode for licensing between Cisco Meeting Management and Smart Licensing Portal must upgrade to version 3.6 and later to continue to use direct mode. If upgrade to version 3.6 is not possible, customers can opt for SLR/PLR mode or on-premise satellite mode. For more information, see [Field Notice for certificate update](#).

---

## 1.6 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](#).

### 1.6.1 End of software maintenance

Table 2: 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 3.5.x	The last date that Cisco Engineering may release any final software maintenance releases or bug fixes for Cisco Meeting Management version 3.5.x is July 15, 2023.

## 1.7 Meeting Management and connected Meeting Servers must run the same software version

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

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 3.7.

### 2.1 Reset Meeting Server Password

From version 3.7, Meeting Management administrators can reset passwords for Meeting Server Admin accounts. In previous releases, if the Meeting Server admin password was forgotten, Meeting Server had to be reinstalled and configured. Administrators can now reset a forgotten or expired password for Meeting Server 1000 and Meeting Server on Virtualized deployments.

Password can be reset using the new **Reset password** button added in the **Edit call bridge** page. While resetting the password, the user is required to provide the previous password for validation. If the user has forgotten the password, they have the option to reset the password without validating the previous password. This can be configured using the new **CMS password reset** option added in the **Advanced security settings** tab. If this option is enabled, the user will not be prompted to enter the previous password while resetting the password.

Follow these steps to reset the password.

1. On the **Servers** page, scroll down to the call bridge and click the **edit** icon.
2. In the **Edit call bridge** page, click the **Reset password** button to launch the **Reset Password** pop-up window. The following fields are displayed:
  - a. **Username** – Displays the username of the MMP administrator.
  - b. **Current password** – Enter the password that is currently configured. This field will not be displayed if the **CMS password reset** option in the Advance security tab is checked. See section for details.
  - c. **New password** – Enter the new password for the Meeting Server. Meeting Management validates the new password against the criteria defined in the Meeting Server and displays error messages in case of invalid entries.
  - d. **Confirm new password** – Re-enter the new password.

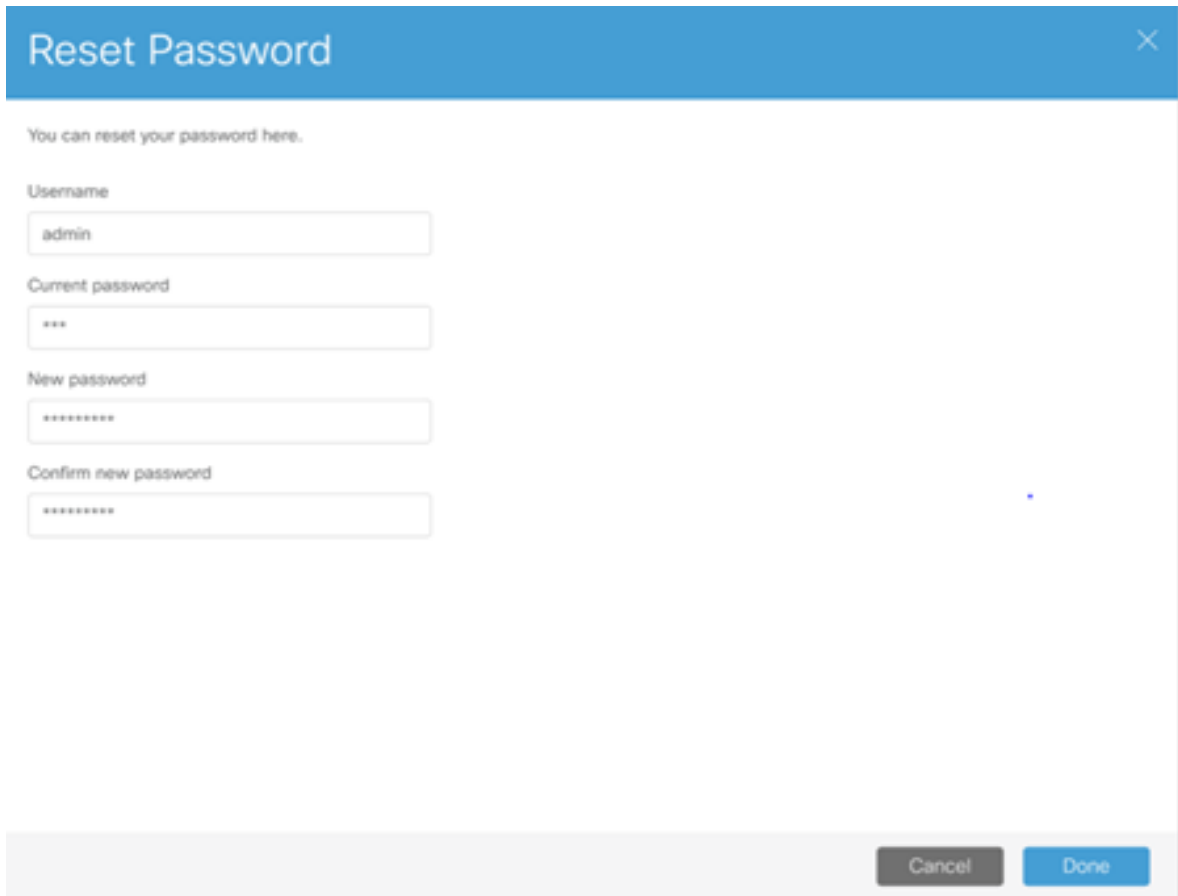


3. Click **Done**.

---

Note: The system validates all fields entered in the reset password pop-up window. Administrators have three attempts to provide valid entries to reset the password, if unsuccessful, they can retry in two hours.

---



Reset Password

You can reset your password here.

Username  
admin

Current password  
\*\*\*

New password  
\*\*\*\*\*

Confirm new password  
\*\*\*\*\*

Cancel Done

4. If the user has forgotten the previous password, configure the below setting to reset the password without validating the previous password:
5. On the **Settings** page, go to **Advanced security** tab.

6. In the **CMS password reset** section, the following setting is displayed:  
**Reset password without validating the previous password** - Check this checkbox to enable password reset without validating the previous password. This option is unchecked by default.

The screenshot shows the Cisco Meeting Management interface. The left sidebar contains navigation options: Overview, Meetings, Spaces, Users, Servers, Logs, Licenses, Settings (selected), and Help. The main content area is titled 'Settings' and 'Advanced security configuration'. It includes sections for 'Sign in rate limiting' (with a checkbox for 'Rate limit sign-in attempts' and input fields for 'Rate at which one token is added to a bucket (in seconds)' set to 300 and 'Maximum number of tokens held in a bucket' set to 3) and 'Idle session timeout' (with a checkbox for 'Idle session timeout' and an input field for 'Time limit after which an inactive user is signed out (in seconds)' set to 3600). The 'CMS password reset' section has a checked checkbox for 'Reset password without validating previous password' and a note: 'Note: CMM administrator logged into the server can change passwords if the previous password validation is removed, which poses an additional security risk.'

7. Click **Save** and restart Meeting Management.

---

Note: The Call Bridge API user credentials section in the Add Server page is now renamed to Admin Credentials. As in the previous releases, this section includes Username, Password and Display name fields.

---

## 2.2 Applying pane placement in custom layouts

Version 3.7 introduces the support for applying pane placements in custom layouts. Administrators and video operators can now place participants in specific panes in a custom layout.

The custom layouts defined in the Meeting Server will be listed in the pane placement window. To apply pane placement, click **Meeting management > Meetings > Pane Placement**. Turn on pane placement to select the custom layout from the list of available layouts and set the pane preference as required.

## Pane placement

Pane placement  On

Select a layout for pane placement

Participants looking at their own pane will see

Add participants to panes

Pane 1	⋮ Reserved. Add Participant	×
Pane 2	⋮ Reserved. Add Participant	×
Pane 3	⋮ Reserved. Add Participant	×
Pane 4	⋮ Reserved. Add Participant	×
Pane 5	⋮ Reserved. Add Participant	×

Add another pane

The screenshot shows the 'Pane placement' configuration window. At the top, there are several layout icons. Below them is a 'Preview' section with a grid of 20 custom layout options, labeled 'Custom 1' through 'Custom 20'. A 'Set layout and pane placement' button is visible at the bottom right of the preview area.

Cancel

Set layout and pane placement

Note: Customizable layouts is a licensed feature. You need to purchase the necessary license for the custom layouts to be listed in the pane placement window.

Pane placement can be applied on a single server or a clustered deployment for ongoing meetings. This feature is supported on web app and SIP end points with single and dual screen endpoints.

## 2.3 Image signing

In previous versions the upgrade images were signed by Meeting Server to enhance the security when upgrading devices. From version 3.7, Meeting Management introduces signatures to Meeting Management upgrade images, and performs verification of the upgrade images (signature and integrity). Meeting Management uses these signatures to verify the authenticity of the upgrade images before each upgrade. This process is done automatically when administrators upgrade to a signed image and removes the need for manual verification.

Meeting Management uses the signatures to confirm whether the image is genuine and rejects the tampered images.

---

Note: Meeting Management does not support secure boot. The signature verification is only performed during an upgrade.

---

Image signatures are verified when upgrading from a signed image only. So, manual verification is still advised when upgrading from an unsigned image to a signed image, i.e., if you upgrade from 3.6 to 3.7, or downgrade to earlier versions, you are still advised to manually verify the hashes. This feature will be fully effective when upgrading from 3.7 and beyond.

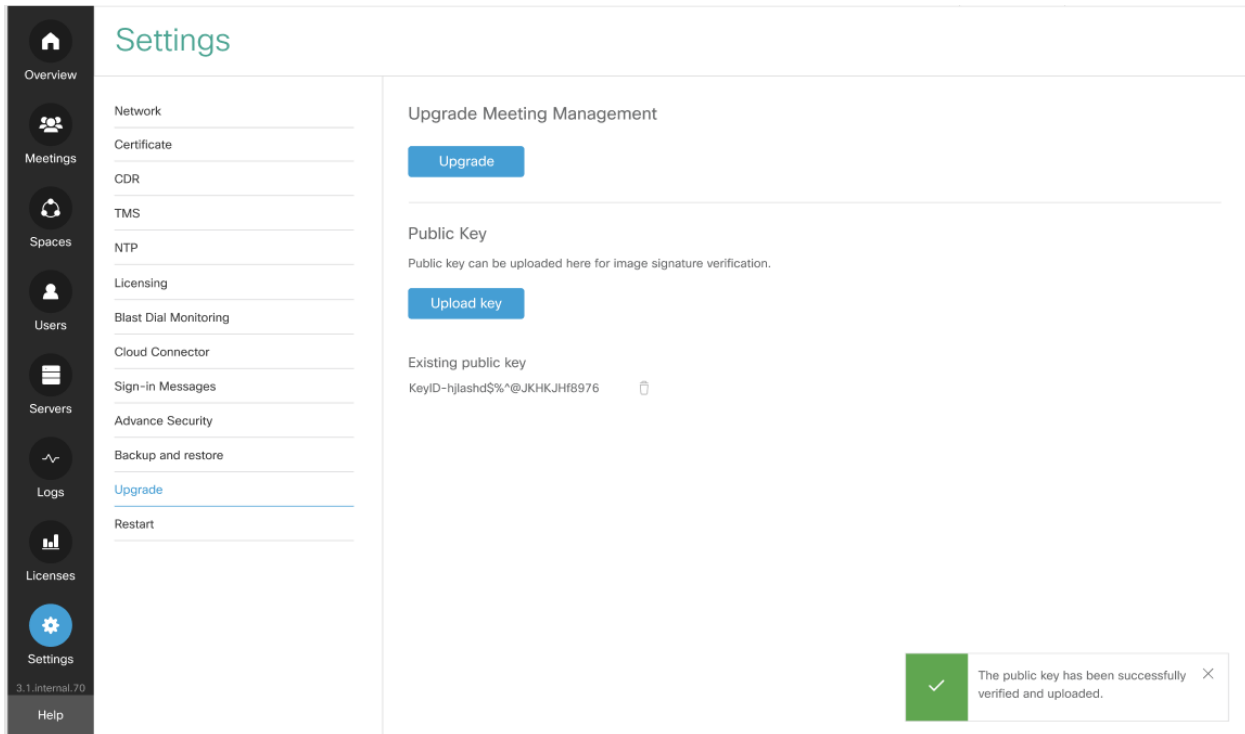
Upgrading from version 3.7, introduces the following differences to the upgrade process:

- Upgrading to a special build will require uploading a special key. A new Upload Key button is introduced to enable administrators to upload the public key and verify the upgrade images. However, the administrators will perform this action only when upgrading to a special build.
- Upgrades from a signed production/ special build to another signed production build will not require any special action from the administrator. Meeting management verifies the upgrade images automatically without the need for manual verification of the hashes.
- On upgrading to an unsigned image, you are warned and asked to confirm whether you want to proceed (this behavior is required for downgrades).
- If the image has been tampered with, the upgrade is prevented.

To upgrade to a special build:

The public key can be uploaded using the **Upload key** button available in the **Upgrade** page. A notification is displayed once the selected public key is verified and uploaded successfully. There is an option to override or delete the uploaded public key.

To upgrade Meeting Management, use **Upgrade** button by navigating to **Upgrade** page in the **Settings** tab. The upgrade file has to be uploaded using the **Upload upgrade file** button available in the **Upgrade** pop-up. Once the upgrade file is uploaded, Meeting Management validates the upgrade image against the uploaded public key.



Note: When upgrading using an Engineering Special release build after the upgrade file is uploaded, Meeting Management validates the upgrade image against the uploaded public key.

**CAUTION:** Upgrading to an untrusted image may compromise the security of your system. Only upgrade to an unsigned image after manually verifying the hashes.

## How image signing works

Upgrade images include a signature generated by a secure internal Cisco server which restricts access to the private key. The public key is stored inside the image of the running Meeting Management and is used to validate signatures. The signature is then used to validate the authenticity of the whole image.

Uploaded public keys are listed below and administrator has an option to delete any uploaded key.

### 2.3.1 Signed image file naming convention

The following convention is used in the image filename:

[release\_name]\_s<s/p><a/b/...>.img

where:

[release\_name]: is the release name

\_s: indicates that the file is signed

<s/p>: indicates if the image is Special/ Production

<a/b/...>: indicates the key version

---

Note: Upgrade images may be renamed before being uploaded to Meeting Management so their names should not be relied upon to determine the image type.

---

### 2.3.2 Key file naming convention

The following convention is used in key filenames:

CMM\_key[\_extra\_info]\_<a/b/...>[\_master]\_<DEV/SPECIAL/RELEASE>.pem

where

[\_extra\_info]: optional key information for SPECIAL keys, to identify the target (EFT, customer name).

<a/b/...>: key version

[\_master]: indicates this is a MASTER key

---

Note: Key files may not be renamed. Renamed keys will be rejected by the Meeting Management.

---

### 2.3.3 File naming examples

Points to note:

- \_spa suffix denotes a production image which will be verified with a key internal to Meeting Management.
- the key version may change if there is a need to rotate the keys.

Only beta or Engineering Special release builds will be signed with a SPECIAL key. Production builds will always be signed with a RELEASE key. Some useful information about builds signed with a SPECIAL key:

- a typical file name example is: upgrade\_ssa.img
- before upgrading to one of these, the SPECIAL key will need to be uploaded to the Meeting Management. Use the **Upload key** option on the **Upgrade** page to add the SPECIAL key.
- upgrades from a release signed with a SPECIAL key to 3.7 or any later release, will not require any special action from the administrator.

## 2.4 Accessibility improvements

In version 3.7, Meeting Management introduces the following accessibility improvements:

- Users can navigate through all the options on the left pane of the main page using arrow keys on keyboard.
- Users can now navigate and access the **Sign out** button under the **Local/admin** option using the keyboard.
- All tabs in the **Users** page now displays meaningful text or symbol to indicate if they are mandatory/required fields.
- The following elements in the Meeting Management are now announced appropriately by the screen reader:
  - Checked/ unchecked checkboxes in **Users** and **Network Settings** pages.
  - UI options such as **Meeting Search** criteria on the **Meetings** page.
  - **Sign In** button on **Login** page.
  - Menu buttons in the **users' profile** option, expanded/ collapsed properties of a button in the **Users** page, and all the toggle buttons in the **Space** page.

## 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/). (<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.

### 3.2 Resolved Issues

Resolved in 3.7 (Build 3.7.0.24)

Reference	Issue
<a href="#">CSCwc76778</a>	The custom layout may not be applied to all participants if a SIP dial-in participant is in the meeting.
<a href="#">CSCwc37612</a>	The custom layout may not be applied to all participants in a meeting with distributed links.



### 3.3 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
<a href="#">CSCwe65616</a>	Taking snapshots is only allowed on CMM for a licensed snapshot version. For the unlicensed version, it returns an error message.
<a href="#">CSCwe53152</a>	During a meeting, Lync participants are unable to take their (own video) snapshots when any of the participants share their screen.
<a href="#">CSCwa37575</a>	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 <b>There is some issue with Authentication file</b> . Refreshing the page shows status of Meeting Management as registered, but in <b>Licenses</b> tab it still displays status as <b>Unlicensed</b> .
<a href="#">CSCwa44321</a>	When collecting logs for servers on the <b>CMS Log Bundle</b> tab, if administrator searches the servers by their name and selects multiple servers, only a single server stands selected.
<a href="#">CSCvz30358</a>	In Meeting Management, while using Installation Assistant to add or configure a new Meeting Server, user can click the disabled <b>Next</b> button in several panels to move to the next panel without configuring the mandatory parameters.
<a href="#">CSCvt64327</a>	If an administrator uses special characters in a template name, then these may appear differently in status messages, displaying escape characters instead.
<a href="#">CSCvt64329</a>	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.
<a href="#">CSCvt64330</a>	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.
<a href="#">CSCvt00011</a>	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.
<a href="#">CSCvr87872</a>	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.
<a href="#">CSCvq73184</a>	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."

---

## 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](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](http://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](http://www.cisco.com/go/offices).

© 2023 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](http://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)