



# Release Notes for Cisco Webex Meetings Server Release 4.0

---

**First Published:** 2019-04-29

**Last Modified:** 2021-06-04

## Release Notes for Cisco Webex Meetings Server

These release notes describe new features, requirements, restrictions, and caveats for all versions of Cisco Webex Meetings Server Release 4.0. These release notes are updated for every maintenance release but not for patches or hot fixes. Each maintenance release includes the features, requirements, restrictions, and bug fixes of the previous releases unless mentioned otherwise. Before you deploy Cisco Webex Meetings Server, we recommend that you review these release notes for information about issues that may affect your system.

New customers can purchase Cisco Webex Meetings Server directly from Cisco Systems, Inc. or from a Partner sales representative.

Existing customers can obtain the Release 4.0 OVA file by using My Cisco Entitlements (MCE): <https://www.cisco.com/c/en/us/products/software/my-cisco-entitlements.html>

To download the latest software updates for this product, visit: <http://software.cisco.com/download>.

Select **Products > Conferencing > Web Conferencing > Webex Meetings Server > Webex Meetings Server 4.0**.

## Finding Documentation

For administration documentation, visit: <http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/tsd-products-support-series-home.html>.

Provide the following URL to your users: <http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-user-guide-list.html>.

## New and Changed Features for Cisco Webex Meetings Server Release 4.0MR4

### CWMS to Cloud Meetings Migration

We've made migrating to the cloud even easier. Use the Cloud Migration Tool to move scheduled meetings to the cloud, so that your users don't have to reschedule them. Provision your users on Cisco Webex cloud, and then use the tool to step through the process. For more information, see the *Administration Guide for Cisco Webex Meetings Server*.

### External Site Warning Message

Participants can now receive an External Site warning message when the host requests to open a website on the participant's computer.

## Restful API Enhancements

Meeting hosts can now send invitations to 500 email addresses. The previous limit was 200. Also, hosts can choose to notify only newly added or removed participants when they edit their meetings.

## Transport Layer Security for Remote Syslog

We've added TLS support for remote Syslog. For information about how to import certificates for remote Syslog, see *Administration Guide for Cisco Webex Meetings*.

## Updated Browser Support

This maintenance release adds support for the following browser versions:

### Microsoft Windows

- Chrome Version: 79–90
- Firefox Version: 71–88

### Mac

- Chrome Version: 79–90
- Firefox Version: 71–88

## Webex Meetings Desktop App

This maintenance release supports Webex Meetings Application version 39.5.27.148 for Mac and Windows.

## Webex Meetings Mobile Application Support

To start and join meetings hosted on a 4.0MR4 site, we strongly recommend that mobile users upgrade their Webex Meeting Mobile applications:

- Webex Meeting Mobile for Android 41.5
- Webex Meeting Mobile for iOS 41.5

## Webex Network Recording Player

This maintenance release supports the following Cisco Network Recording Player versions:

- **Windows:** 39.5.27.148
- **Mac:** 39.5.27.148 (online), 39.05.21.00 (offline)

You can install the latest version from the **Downloads** page of your Cisco WebEx site. When you download the Cisco Network Recording Player, select **Windows** or **Mac** from the operating system drop-down list. The Windows player is the default download.

## What's New in Cisco Webex Meetings Server Release 4.0MR3

This section describes what is new for Cisco Webex Meetings Server Release 4.0MR3.



---

**Important** The 4.0MR3 software update is only for systems that are currently running Cisco Webex Meetings Server build 3.0.1.3119 and later, 4.0.1.19 and later, 4.0.1.1110 and later, or 4.0.1.2147 and later.

For information about important new upgrade considerations, see the following topics:

- [Supported Ciphers, on page 20](#)
  - [Webex Productivity Tools, on page 8](#)
  - [Supported Upgrade Paths, on page 14](#)
- 

### 4.0MR3 Security Patch 3

We've updated the following components:

- Webex Meetings Client 39.5.27.43
- Network Recording Player 39.5.27.43
- Webex Meetings desktop app 39.5.27.43

We've also added support for TFS and URL-Protocol, for starting meetings and playing NBR recordings.

This patch introduces support for MacOS 11, Big Sur.

### Meeting Search Export Enhancement

We've enhanced Meeting Search functionality so that your exported .CSV files contain more information. The new fields are:

- **Alternate Host ID**
- **Create Time**
- **Creator ID**
- **Duration**
- **End Time**
- **Expiration Type**
- **Host ID**
- **Host Type**
- **Last Modified**
- **Meeting ID**
- **Participants**
- **Password protected (Yes/No)**
- **Repeat Type**
- **Start Time**

## Modern View Enhancements

For more information about the following features, see *User Guide for Cisco Webex Meetings Server Release 4.0*.

### Meeting Details Page

The list of attendees appears in the **Who Is Invited** section. Hosts can assign attendees as alternate hosts, or remove the alternate host privilege.

### Modern View Preferences

Modern View users can go to **Preferences** and select **Audio** to set their **Host PIN**. Users can also create and manage access codes, for up to three Personal Conferencing accounts.

Host can go to **Preferences** and select **Scheduling** to choose their preferred **Meeting type**. Hosts can also grant other hosts permission to schedule meetings on their behalf.

### Modern View Scheduling

We've improved the **Schedule a Meeting** page. Hosts can configure the following new **Advanced options**:

- **Meeting type**
- **Audio connection options**
  - **Audio connection type**
  - **Entry and exit tone**
- **Scheduling Options**
  - **Automatic recording**
  - **Exclude password**

### Predictive Search

When users type an email address to add an attendee, predictive search displays suggestions.

### Recorded Meetings List Support

Modern View users can now select **Recordings** to see a list of their meeting recordings. From the **My Recorded Meetings** page, users can play, download, and manage their meeting recordings. They can also search for Personal Rooms.

### Download the Webex Network Recording Player

Modern View now offers the option to download the Network Recording Player.

## Monitoring and Reporting Disk Usage

Cisco Webex Meetings Server monitors disk partition size and usage for all virtual machines (VM). If usage exceeds 90% of the partition size for a VM, the system sends email notifications to all administrators.

## Monitoring and Reporting Storage Health

Cisco Webex Meetings Server monitors storage health and availability for all VMs in the system, except the IRP VMs. If the system detects that storage for a VM isn't reachable, CWMS sends emails to all administrators to notify them about the problem.

## Personal Room Autolock Settings

We've enhanced security for Personal Rooms. Users can set their Personal Room to lock automatically—0, 5, 10, 15, or 20 minutes after their meetings start. For more information, see *User Guide for Cisco Webex Meetings Server Release 4.0*.

We've also added new Site Administration settings. You can enable the automatic locking feature for all users who haven't defined their autolock preference. You can also prevent users from changing their autolock preference. For more information, see *Administration Guide for Cisco Webex Meetings Server Release 4.0*.

## Updated Browser Support

This maintenance release adds support for the following browser versions:

### Microsoft Windows

- Chrome Version: 79 and 80
- Firefox Version: 71, 72, 73, and 74

### Mac

- Chrome Version: 79 and 80
- Firefox Version: 71, 72, 73, and 74

## Updated CUCM Support

This maintenance release adds support for Cisco Unified Communications Manager Release 11.5 SU7, 11.5 SU8, and 12.5 SU2.

## Webex Meetings Desktop App

This maintenance release supports Webex Meetings desktop app versions 39.5.21.10 for Mac and for Windows.

## Webex Meetings Desktop App Enhancement for Personal Rooms

We've made it easier to use the Webex Meetings desktop app to join meetings in Personal Rooms. Users can now enter the meeting host's Personal Room ID to start or to join their meeting. For more information, see *User Guide for Cisco Webex Meetings Server Release 4.0*.

## Webex Meetings Mobile Application Support

We strongly recommend that users upgrade their Cisco Webex Meetings mobile app for iOS or Android to version 40.2.

## Webex Meetings Security Enhancement

We've enabled the **End meeting when host and all authenticated participants leave** option by default. To disable this feature, clear the checkbox. For more information, see *Administration Guide for Cisco Webex Meetings Server Release 4.0*.

## Webex Network Recording Player

This maintenance release supports the following Cisco Network Recording Player versions:

- **Windows:** 39.5.21.10
- **Mac:** 39.5.21.10 (online), 39.05.21.00 (offline)

You can install the latest version from the **Downloads** page of your Cisco WebEx site. When you download the Cisco Network Recording Player, select **Windows** or **Mac** from the operating system drop-down list. The Windows player is the default download.

## What's New in Cisco Webex Meetings Server Release 4.0MR2

This section describes what is new for Cisco Webex Meetings Server Release 4.0MR2.




---

**Important** The 4.0MR2 software update is only for systems that are currently running Cisco Webex Meetings Server Release 4.0.1.19 and later, or 4.0.1.1110 and later.

For information about important new upgrade considerations, see [Webex Productivity Tools, on page 8](#) and [Supported Upgrade Paths, on page 14](#).

---

## Health Checker for Mac

To match the functionality available for Microsoft Windows, this maintenance release includes Health Checker for Mac.

## Reduced Requirements for Maintenance Mode

To help reduce system downtime, we've further reduced the number of audio settings that require Maintenance Mode for changes. Put the system into Maintenance Mode to change the following audio settings:

- Voice connection using computer
- Transport
- Port Number
- IPv6 Teleconferencing
- System Audio Language

You can change any of the other audio settings, without putting the system into maintenance mode.

## Removal of Special Character Support

Webex follows a new approach to generating Personal Room IDs. If a Personal Room ID contains special characters (non-Latin codes), Webex drops the special characters in the string, and keeps only the valid characters.

If the resulting Personal Room ID exists in the system, Webex appends a number to create a unique ID.

For example, “p&hil” become “phil”. If "phil" is in use, the system changes it to something like “phil423”.

## Monitor VM Time Synchronization

Cisco Webex Meetings Server now monitors time synchronization for each virtual machine (VM) in the deployment. The primary Admin VM controls and runs the monitoring process every five minutes. The time difference between the primary Admin VM, and any other VM in the deployment, should be less than five seconds. If the time difference is more than five seconds, the system sends an email alert to all Administrators. The email specifies which VM has the problem and what to do, to avoid issues. The system sends an email alert every four hours, until the problem is fixed. This feature can help you to avoid many issues caused by time synchronization problems.

## Optimized Grid-View for Low Bandwidth

A low-bandwidth warning appears if your network connection falls below the minimum requirements for video. During low-bandwidth conditions, you may not receive all participant video streams. Prior to this release, the available streams appeared sporadically in the grid view. Cisco Webex Meetings Server now prioritizes the available video streams at the top of the grid.

## Updated Browser Support

This maintenance release adds support for the following browsers:

### Microsoft Windows

- Chrome versions 77 and 78
- Firefox versions 69 and 70

### Mac

- Chrome versions 77 and 78
- Firefox versions 69 and 70
- Safari version 13

## Updated CUCM Support

This maintenance release adds support for Cisco Unified Communications Manager Release 12.5 and Release 12.5(1) SU1.

## Updated macOS Support

We've added support for macOS Catalina (Version 10.15).

## Webex Meetings Desktop App

This maintenance release supports Webex Meetings Application version 39.5.15.4 for Mac and Windows.

## Webex Network Recording Player

This maintenance release supports the following Cisco Network Recording Player versions:

- **Windows:** 39.5.15.4

- **Mac:** 39.5.15.4 (online), 39.05.12.00 (offline)

You can install the latest version from the **Downloads** page of your Cisco Webex site. When you download the Cisco Network Recording Player, select **Windows** or **Mac** from the operating system drop-down list. The Windows player is the default download.

## Webex Productivity Tools

The Webex Meetings desktop app replaced Webex Productivity Tools for Cisco Webex Meetings Server 4.0. However, if you need to use Productivity Tools as part of your upgrade strategy, only version 2.82.7000.1229 or later is compatible.

## What's New in Cisco Webex Meetings Server Release 4.0MR1

This section describes what is new for Cisco Webex Meetings Server Release 4.0MR1.




---

**Important** The 4.0MR1 software update is only for systems that are currently running Cisco Webex Meetings Server Release 4.0.1.19 and later.

---

### Administrative XML Web Service Failover

We have added a background job to support Administrative XML Web Service (AXL) failover. This feature ensures that if the CUCM Publisher goes down and CUCM subscribers takes over AXL service, CWMS automatically switches to subscribers. This feature eliminates the need to change the LDAP integration for CUCM in Webex Site Administration.

### Cisco Webex Meeting Mobile Version

To start and join meetings hosted on a 4.0MR1 site, we strongly recommend that mobile users upgrade their Webex Meeting Mobile applications:

- Webex Meeting Mobile for Android 39.6
- Webex Meeting Mobile for iOS 39.6

### Health Checker

The in-meeting Health Checker provides an intuitive and easy way to understand the status of your meeting and system performance.

The Connection and Device status indicators are green (good), yellow (there may be potential issues), or red (issues have been found). You can hover over the status for more details. You can even send a problem report directly from the Health Checker. We moved the Audio & Video Statistics link from the Meeting menu to the Health Checker.

When the Health Checker identifies a problem, it provides a summary of the problem and a list of actions that you can take to help solve the problem.

### Problem Reporting for Mac OS

This release adds Mac support for Cisco Webex Meetings Problem Reporting. If Mac users experience issues with the Webex Meetings desktop app, they can generate problem reports to assist with troubleshooting.



To generate a report, open the Webex Meetings desktop app and go to **Help > Send Problem Report**.

## Restart and Exit Maintenance Mode

After updating the system, Administrators can choose between the following options:

- **Restart**—Restarts the system and requires that an Administrator manually turn off maintenance mode.
- **Restart & Exit Maintenance**—Restarts the system and turns off maintenance mode, which saves time.

## Sign-in History

Modern View provides users with a summary of their sign-in activity, which includes:

- The IP address for their last sign-in
- The time of their last sign-in
- The time of their last sign-out
- The number of unsuccessful sign-in attempts since their last successful sign-in

## Take Virtual Machine Snapshots

You can use Webex Site Administration to take snapshots of the system virtual machines. After you put the system in maintenance mode, and specify the vCenter URL and credentials, you can take a snapshot of each virtual machine in a vCenter. If your IRP virtual machines are in another vCenter, you can specify the URL and credentials for the other vCenter and take all snapshots at the same time.

Using vSphere Data Protection to take snapshots is still supported.

## Updated Browser Support

This maintenance release adds support for the following browsers:

### Microsoft Windows

- Google Chrome: 75 and 76
- Mozilla Firefox: 67 and 68

### Mac

- Google Chrome: 75 and 76
- Mozilla Firefox: 67 and 68

## Updated vCenter ESXi Support

This maintenance release supports vCenter ESXi 6.5 and 6.7.

## Use as Guest

Users who don't have a Webex account, or who haven't signed in to their accounts can use the Webex Meetings desktop app as guests. Guest users can join meetings by using one of the following methods:

- Enter the meeting link, or video address

- Click the **Join** button for the meeting (in the **Upcoming Meetings** list)

### Limitations

Guest users cannot join meetings by meeting number. The Webex Meetings desktop app does not support joining Personal Room meetings.

## Webex Meetings Desktop App

This maintenance release supports Webex Meetings desktop app version 39.5.11.7 for Windows and Mac.

## Webex Network Recording Player

This maintenance release supports the following Webex Network Recording Player versions:

- **Windows:** 39.5.11.7
- **Mac:** 39.5.11.7

## What's New in Cisco Webex Meetings Server Release 4.0

This section describes features that are new or changed in this release.




---

**Important** [Smart Licensing, on page 13](#) is a significant change for this release, because it completely replaces traditional license management.

---

For a complete list of system requirements, see the *Cisco Webex Meetings Server Planning Guide and System Requirements Release 4.0*. Visit [http://www.cisco.com/en/US/products/ps12732/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html).

## 64-Bit Application Support for Mac

Apple has announced end-of-support for 32-bit applications; macOS High Sierra will be the last macOS release to support 32-bit architecture. The Webex Meetings Desktop Application is a 64-bit application.

## Avatar Support for Mobile

Mobile users can upload avatars (images) to the site, for display on the Webex site, in the Webex Meetings desktop app, and in their mobile app.




---

**Note** Currently, users must sign in to their Webex site (in Classic View or Modern View) to upload the avatar image. The mobile apps do not support uploading avatars.

---

Image files must meet the following requirements:

- Supported file formats: PNG, JPG, JPEG, and GIF
  - Animated GIFs are supported, but the system converts them to static images and uses the first frame as the avatar image.
- Minimum image dimensions: 160 x 160 pixels

- Maximum image size: 5MB

This feature requires that you have remote storage installed. The system stores avatars on the Admin server in /db/archive/avatars/.




---

**Note** Multi-data Center systems replicate the avatars images from one data center to the other.

---

## Browser Support

This release supports the following browser versions:

### Windows:

- Google Chrome: 65, 66, 67, 68, 69, 70, 71, 72, 73, and 74
- Microsoft Edge (Windows 10 only): 42.17134.1.0 and 44.17763.1.0
- Microsoft Internet Explorer (IE): 11
- Mozilla Firefox: 59, 60, 61, 62, 63, 64, 65, and 66

### Mac:

- Apple Safari: 12.0.1 (14606.2.104.1.1) and 12.1
- Google Chrome: 65, 66, 67, 68, 69, 70, 71, 72, 73, and 74
- Mozilla Firefox: 59, 60, 61, 62, 63, 64, 65, and 66

## Cisco Jabber Support

This release supports Cisco Jabber Release 12.1.0, 12.1.1, 12.5.0, and 12.6.0.

## Cisco Unified Communications Manager Support

This release supports Cisco Unified Communications Manager (CUCM) 8.6 or 9.0 without TLS/SRTP, and CUCM 9.1, 10.0, 10.5, 11.0(1a), 11.5(1)SU1, 11.5(1)SU3, 11.5SU5, 11.5SU6, 12.0, 12.0SU2, and 12.5 for secure teleconferencing.

## Display Caller ID

You can enable or disable the display of the Caller ID in the Participants panel, for call-in users. To toggle this feature on or off, sign in to Webex Administration and go to **Settings > Meetings > Meeting Settings**. By default, this feature is disabled.

When the feature is disabled, the ID for a call-in user appears as: Call-in User\_#. Examples:

- Call-in User\_1
- Call-in User\_2
- Call-in User\_3

When the feature is enabled, the ID for a call-in user appears as: Call-In User\_# (<caller ID>). Examples:

- Call-in User\_1 (Giacomo Edwards +865516611\*\*\*\*)

- Call-in User\_2 (WIRELESS CALLER +1650400\*\*\*\*)
- Call-in User\_3 (MARC BROWN +1917929\*\*\*\*)



---

**Note** For privacy reasons, the last four digits are masked by asterisks. The display supports up to 63 characters.

---

## Extended Capacity for Multi-data Centers

Cisco Webex Meetings Server supports a fully-functional 4000 port system, for the following scenarios:

- Single Data Center with High Availability (HA), using VMware V-Center 6.5
- Multi-Data Center (MDC)—Dual Data Center (DDC), using VMware V-Center 6.5

Both the Extended Capacity and MDC features are available for Release 3.0; but not supported together. This release adds support for two extra large (4000 port) systems, joined to create an MDC. If you already have a large MDC system, you can extend both systems to create an extra large MDC system.

The Extended Capacity feature requires a license for each system. The Extended Capacity license is available only for large (2000 port) systems.

## macOS Support

This release supports the following macOS versions:

- Sierra 10.12.6
- High Sierra 10.13.6
- Mojave 10.14.1
- Mojave 10.14.2
- Mojave 10.14.3
- Mojave 10.14.4

## Modern View

When users sign in to the Webex site, they can choose between Classic and Modern View. With Modern View, they can access the most commonly used site controls directly from a new dashboard. Users can easily start Webex Personal Room meetings, join upcoming meetings, and schedule new meetings.

In Modern View, the dashboard is the home page. Users can return to it at any time by selecting on the left navigation bar. Modern View appears by default, but you can change the default for your Webex site.

## Personal Meeting Rooms

Webex Personal Rooms are virtual conference spaces that are always available. The Personal Room URL and call-in numbers stay the same. Users can set their own preferences for their Personal Rooms, start instant meetings, and share the links to meet right away.

## Smart Licensing

This release introduces Smart Software Licensing, which greatly simplifies all aspects of licence management. For more information about the benefits of Smart Software Licensing, see the following resources:

**FAQ:** <https://www.cisco.com/c/dam/en/us/products/collateral/software/smart-accounts/q-and-a-c67-741561.pdf>

**At-a-Glance:** <https://www.cisco.com/c/dam/en/us/products/collateral/ssl-aag.pdf>

For more information about license management and how to get started, see "Managing Licenses" in the *Administration Guide for Cisco Webex Meetings Server*:

<https://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html>

## Webex Meetings Desktop App

The Webex Meetings desktop app replaces the Webex Meeting application and Productivity Tools. The Webex Meetings desktop app adds new video features, and support for Personal Meeting Rooms.

Cisco Webex Meetings Server supports the Webex Meetings desktop app version 39.3.0.582 for Windows and Mac.



**Attention** Scheduling and editing meetings from Microsoft Outlook for Mac is not supported. As a workaround, users can schedule, edit, and start meetings from your Webex site.

**Table 1: Webex Meetings Desktop App Video Features**

Feature	Description
Video thumbnails	Video-based participant list with video thumbnails.
Video self-view in full-screen sharing view	View self-view video in the main video display when sharing in full-screen view. Start or stop sending video from the self-view video window.
Up to high-definition resolution (720p)	Video resolution can go up to high-definition 720p resolution (1280x720).
Lock video	Presenter can determine whose video will be displayed to all participants.
High-definition video decode offloading to GPU	Supported GPU chipsets can offload decode processing from the host CPU.
Full-screen video view	Full-screen video view with high-definition or high-quality video display (depending on monitor size) and five video thumbnails.
Expanded full-screen video view	Expand the active speaker to the whole screen, which also allows high-definition video to be received.
Camera hot plug-in	Attendees can connect and switch web cams while in a meeting.
Auto-adjust Video	Automatic configuration of participants' video quality according to available network bandwidth.

Feature	Description
Active speaker video display in full-screen sharing view	Floating active speaker video display when sharing in full-screen view.
Active speaker switching	Automatic video switching to the loudest active speaker.

Updates to the Webex Meetings desktop app may be made available in the form of Patches, Maintenance Releases, and Hotfixes.




---

**Attention** If your users also connect to Cloud-based Webex sites, they could update the Webex Meetings desktop app from those sites. The updated version will work with Cisco Webex Meetings Server. The site to which the user connects determines the available feature set.

---

## Webex Network Recording Player

This release supports the following Cisco Network Recording Player versions:

- **Windows:** 39.3.0.582
- **Mac:** 39.3.0.582

## Supported Upgrade Paths

This release of Cisco Webex Meetings Server supports upgrades from release 1.5 to 3.0. The following points apply:

- An upgrade is a replacement of the system to deploy major modifications that we made to the system.
- An update is an incremental modification of the system. Updates deploy fixes and minor improvements.
- An update retains all data from the original system. An upgrade retains all data from the original system, except for the logs.
- You can't change the audio encryption type (Audio Encrypted -AE/Audio Unencrypted -AU) for the system, during an upgrade or during an update. After deployment, the only way to change a system from one type of audio encryption to the other is to deploy a new system.
- When upgrading, you can't skip a major version of the software and go directly to a companion maintenance release (MR). For more information, see the following table.

Use the following table to determine your upgrade path to Cisco Webex Meetings Server Release 4.0.

Installed Release	Path to Release 4.0 <sup>1</sup>
2.8 <sup>2</sup>	<ol style="list-style-type: none"> <li>1. Update to the latest available 2.8MR3 patch.</li> <li>2. Install Webex Productivity Tools, or push it to the desktops.</li> <li>3. Upgrade to 4.0 FCS.</li> <li>4. Update to the latest available 4.0MR release and patch.</li> <li>5. Uninstall Webex Productivity Tools.</li> <li>6. Install the Webex Meetings desktop app, or push it to the desktops.</li> </ol>
3.0 <sup>3</sup>	<ol style="list-style-type: none"> <li>1. Update to the latest available 4.0MR and patch.</li> <li>2. Uninstall Webex Productivity Tools.</li> <li>3. Install the Webex Meetings desktop app, or push it to the desktops.</li> </ol> <p><b>Important</b> You can't start instant meeting from Webex Productivity Tools versions earlier than 2.82.7000.1229.</p>
4.0	<ol style="list-style-type: none"> <li>1. Update to the latest available 4.0MR and patch.</li> <li>2. Update Webex Meetings Desktop app if required.</li> </ol>

<sup>1</sup> The Webex Meetings desktop app replaced Webex Productivity Tools for Cisco Webex Meetings Server 4.0. If you require Productivity Tools as part of your upgrade strategy, only version 2.82.7000.1229 or later is compatible.

<sup>2</sup> If your system is running an earlier version, see the *Release Notes for Cisco Webex Meetings Server Release 2.8*.

<sup>3</sup> The Webex Productivity Tools version must be 2.82.7000.1229 or later, to start the 4.0 and later meeting clients. Upgrade Productivity Tools, before you update Cisco Webex Meetings Server to 4.0MR2.



**Note** All updates require downtime. For Multi-data centers, you update both data centers simultaneously.



**Caution** Don't click **Restart** for one data center until the update for the other is complete, and both display the **Restart** button.

## Updating Your High-Availability System

For systems with an existing High Availability (HA) system already attached, the HA system automatically updates when you update the primary system. Ensure that all HA virtual machines are turned on and running before you start the update process.

To add a High Availability (HA) system to your primary system, first deploy the HA system. Then update the HA system to the same version as the primary system. The HA system restarts at the end of the update

process. We recommend that you wait an extra 15 minutes after the restart, before you begin to add the HA system to the primary system.

For more information, see the *Cisco Webex Meetings Server Administration Guide* for your release:

<http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html>

## Limitations and Restrictions

### Audio-only Meetings

Under the following circumstances, a meeting can continue for more than the 24-hour maximum meeting duration:

- All attendees for a regular Webex meeting are dial in (audio-only).
- No attendee starts the web portion of the meeting.

In this case, the meeting continues as long as one attendee remains in the conference. If all dial-in attendees disconnect from the conference, the meeting ends within 24 hours of the start time. The meeting ends immediately if the meeting ran past the scheduled end time.



---

**Note** This scenario applies only to regular Webex meetings joined only by dial-in participants. This scenario does not apply to Personal Conference Number (PCN) meetings, or to regular Webex meetings joined by web participants.

---

### Internet Reverse Proxy Removal

As part of the Internet Reverse Proxy (IRP) node removal process, the Admin virtual machine sends a remove message to the IRP server. The message removes the IRP server and therefore all external access to the system. The message is sent as clear text, and it is unauthenticated. Well-crafted malicious code could replicate this behavior and lead to a denial of service.

We recommend that you limit access to port 64616, on the IRP node, to the Admin virtual machine only.

### macOS 11.x Big Sur

CWMS supports macOS 11.x, subject to the following limitations:

- The Webex Meetings client application for CWMS isn't designed for macOS 11.x. We tested for compatibility and made fixes to provide best-effort support.
- M1 chip support is pending validation testing.

### Microsoft Edge Browser

The Microsoft Edge browser does not support the playback of Webex recordings.

### Recording Limitations

The maximum recording size, per recording, is 2.2 GB (existing system limit). For Multi-data Centers, ensure that there is sufficient storage capacity available for all data centers. The maximum number of recordings



depends on your storage server capacity. You can estimate the required storage server size for a typical five-year period using the following formula:

Estimated hours of meetings that you expect to be recorded per day \* 50-100 MB per hour of recording \* five years \* 24 hours per day \* 365 days per year

There are no per-user storage limitations. The system stores recordings indefinitely until users delete them. To prevent important recordings from being accidentally deleted, there is no setting to enable the automatic deleting of recordings. The storage server retains recordings marked for deletion for up to six months. During that time, users can still archive the recordings to other media.

When you configure a storage server and check **Record** under **Administration Dashboard > Settings > Meetings > Participant Privileges**, the **Record** setting is a system-wide setting. There are no individual meeting settings or preferences for recordings. You can also enable or disable recording by Session Types, which you assign to users.

## Session Types

A session type is a predefined bundle of features and options (a profile) that site administrators can customize and assign to users. The default session (meeting) type is the PRO session type. Because of the relationships between the PRO session type and the custom session types, we recommend that you do not modify the PRO session type. The best practice is to create a custom session type to modify.

## SSO and Email Address Changes

With this release, the Identity Provider (IdP) server can use any unique and static Active Directory (AD) field as the NameID for SSO configuration. If you plan to use the email address change feature, the email AD field is not static. Change the mapping for the NameID field on the IdP server to a unique AD field other than email. If you do not plan to use the feature to change email addresses, there is no requirement to change the mapping for the NameID field.



### Caution

If the NameID field is mapped to the email AD field and you change user email addresses, the system creates a new user account for each changed address.

If you plan to change the NameID field mapping from email to another field (such as EmployeeNumber), users must prepare for the change. After you update the NameID fields in AD, have the users log in to CWSM before you change the email addresses. Otherwise, when both the NameID and email address change, no attribute matches the CWMS profile. In this scenario, the existing profile loses the ability to log into the system and the system creates a new profile.

Outlook synchronizes with the Exchange server once a day. If you change an existing user's email address on the Exchange server, the change does not immediately propagate to Outlook. Until synchronization occurs, the system receives the user's former email address and issues a notice that the user cannot be found. A delegate (proxy) user cannot schedule a meeting for the user, or identify them as an alternate host, until after Outlook synchronizes with the Exchange server.

Manually synchronizing the systems does not solve this issue. This limitation is not a CWMS issue; it is the result of Outlook and Exchange design.

See also [About SSO Configuration, on page 21](#).

## TLS Support

This release supports TLS 1.1 and later; TLS 1.0 is not supported, with one exception. Client connections from Cisco Webex Meetings Server (CWMS) to an SMTP server using TLS 1.0 are supported.

## vCenter 6.5 Support

When you deploy the CWMS OVA file on vCenter 6.5, the following restrictions apply:

- Because of browser limitations and the CWMS OVA file size of 16GB, you must deploy the OVA file by using the URL and not the local file upload.
- Choose the vCenter FLASH based client. This selection is required to successfully populate the vApp properties for VM configuration: hostname, domain, IP address, subnet and DNS configuration.

## Virtual Desktop Infrastructure

The following limitations and restrictions are known to affect virtual desktop infrastructure (VDI) environments.

- Citrix Virtual Apps and Desktops is the only desktop virtualization software supported for this release of Cisco Webex Meetings Server.
- An architectural limitation of the virtual desktop environment can affect video quality. The frame rate may be low, causing a suboptimal experience when sending video.
- Some video files cannot be shared in a virtual desktop environment.
- Remote Access and Access Anywhere are not supported in virtual desktop environments. The underlying Citrix platform removes the Remote Access and Access Anywhere agents after the operating system restarts.

## Webex Meetings Desktop Application

The Webex Meetings Desktop Application has the following limitations. Users cannot perform the following actions:

- Schedule a yearly meeting.
- Join a meeting using a video address.
- Schedule or join Personal Room meetings from the Webex Meetings Desktop Application.
- Schedule Personal Room meetings from Microsoft Outlook.
- Connect and join meetings from video devices.
- Connect and share to cloud-registered video devices.
- Connect and share to Webex Share devices.
- Receive a callback to a video device during a meeting (Call My Video System).
- Start or join a meeting from Microsoft Word, PowerPoint, or Excel.




---

### Attention

Scheduling and editing meetings from Microsoft Outlook for Mac is not supported. As a workaround, users can schedule, edit, and start meetings from your Webex site.

---

## Upgrade Considerations

The Webex Meetings Desktop Application is not backwards-compatible with earlier versions of Cisco Webex Meetings Server.

After you upgrade your system to CWMS 4.0, you can choose whether to push the application to end users, or to permit them to download it themselves.

If you push the Webex Meetings Desktop Application to users, they must sign in to the application with their existing credentials. This is true, even if they previously chose the remember me and auto sign-in options for Webex Productivity Tools.

If you permit users to download and install the application themselves, Microsoft Windows users must first uninstall Webex Productivity Tools.

If permitted, some users may opt to continue using Webex Productivity Tools. These users will not be able to start instant meetings by clicking the **Start Meeting** button. A hotfix is available to fix this issue.

## Important Notes

### About Using Self-Signed Certificates

We strongly recommend using a publicly signed certificate instead of the provided self-signed certificate. User's browsers trust publicly signed certificates because the list of Root Certificate Authority certificates installed on the computer establishes trust.

For Multi-data Center systems using self-signed certificates, the user receives multiple certificate warnings and must trust and install all certificates to use the system.

When using self-signed certificates, some users might have difficulty joining meetings because browsers by default do not trust such certificates. Users are required to explicitly establish trust in this case before they can proceed to join a meeting on your site. Some users might not understand how to establish trust with such a certificate. Others might be prevented from doing so by administrative settings. Use publicly signed certificates whenever possible to provide the best user experience.

The User Guide provides more information about this issue for users. See the "Meeting Client Does Not Load" topic in the "Troubleshooting" chapter of the *Cisco Webex Meetings Server User Guide* at [http://www.cisco.com/en/us/products/ps12732/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/us/products/ps12732/products_user_guide_list.html).

### Hypervisor Support

Cisco Webex Meetings Server runs on VMware virtual machines.

- Both VMware vSphere and VMware vCenter are required to deploy Cisco Webex Meetings Server. Using the vSphere client, you deploy the Cisco Webex Meetings Server OVA file on an ESXi host managed by vCenter.
- Purchase VMware vSphere 5.5, 6.0, or 6.5 for use as the hypervisor platform for Cisco Webex Meetings Server.
  - Buy vSphere directly from Cisco on the GPL (Global Price List). Cisco is an approved VMware partner and distributor. This is convenient for those who want to purchase everything from a single vendor.
  - Purchase vSphere directly from VMware, through enterprise agreements you have directly with VMware.

- Cisco Webex Meetings Server does not support other hypervisors.
- For more information about hypervisor requirements, see the *Planning Guide and System Requirements for Cisco Webex Meetings Server* at [http://www.cisco.com/en/US/products/ps12732/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html).

## Supported Ciphers

Cisco Webex Meetings Server supports the following ciphers:

### TLS Version 1.1

- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (secp256r1)
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (rsa 2048)
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (rsa 2048)

### TLS Version 1.2

- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (secp256r1)
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (secp256r1)
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (secp256r1)
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (rsa 2048)
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 (secp256r1)
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (secp256r1)
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (rsa 2048)
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (rsa 2048)
- TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (rsa 2048)
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (rsa 2048)
- TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (rsa 2048)

### SRTP SIP Call Signaling

Cisco Webex Meetings Server also supports the following crypto ciphers for SRTP calls over SIP line and SIP trunk:

- AEAD\_AES\_128\_GCM  
*AEAD* is Authenticated-Encryption with Associated-Data, and *GCM* is Galois/Counter Mode.
- AEAD\_AES\_256\_GCM
- AES\_CM\_128\_HMAC\_SHA1\_80
- AES\_CM\_128\_HMAC\_SHA1\_32




---

**Important** If you have SRTP and AES-GCM configured, check the firmware versions for your IP Phones, before you upgrade to Cisco Webex Meetings Server Release 4.0MR3. Ensure that the IP Phones have the latest firmware—version 12.7.1 or later, or 14.0.1 or later, depending on the model.

---

## About SSO Configuration

This release supports using any unique Active Directory (AD) field as NameID for SSO configuration. We recommend following AD attributes for NameID for SSO configuration:

- Email
- SAMAccountName
- UserPrincipalName (UPN)
- TelephoneNumber
- EmployeeNumber
- ObjectSid

## Mandatory SAML Assertion Attributes

The following SAML assertion attributes are required for the Auto Account Creation feature:

- lastname
- firstname
- email




---

**Important** The email attribute is always required, even if Auto Account Creation and Auto Account Update are disabled in the SSO configuration.

---

## Expanding Your System

If you have VMware snapshots on your existing (pre-expansion) system, remove them before beginning the expansion.

System expansion requires Virtual Machine Disk (VMDK) attaching, from the original system to the target (expanded) system. If you leave snapshots on the original system and attach it to the target system, the target system won't power on because of snapshot inconsistency.

## SNMP v2 Community Names

There is no default SNMP v2 community name entry in this release of Cisco Webex Meetings Server. The system will remove the existing Cisco Webex Meetings Server 1.0 default Community Name, "CWS-Public," after upgrading. Only user-added SNMP v2 community names are maintained.

## Translated Documentation

Translated documentation for this release of Cisco Webex Meetings Server is published 4–6 weeks after the English-language release.

## Known Issues and Notices

### Apple iOS 6.x and SSO

There is a known issue with Apple iOS 6.x. Single sign-on (SSO) does not work for internal users of iPad/iPhone who are using the Safari 6 web browser. An Apple defect that is fixed in iOS 7 caused this issue. The Safari bug ID is 13484525.

### Audio Configuration

On your audio configuration settings, G.711 provides better voice quality than G.729. See “About Configuring Your Audio Settings” in the *Cisco Webex Meetings Server Administration Guide* for more information.

### Cannot Share .mp4 Video File Format on Windows

When using QuickTime, the following message may appear: “QuickTime failed to initialize. Error # –2093. Please make sure QuickTime is properly installed on this computer.”

This error message can indicate that the file QuickTime.qts is missing, moved, or unusable. The QuickTime.qts file is located in the \WINDOWS\SYSTEM directory. To resolve this symptom, completely remove and reinstall QuickTime.

1. Download the latest version of the QuickTime Player <http://www.apple.com/quicktime/download/>.
2. Uninstall QuickTime using the **Add or Remove Programs** control panel. Ensure that you select **Uninstall Everything**.
3. Delete the contents of the Temp folder, C:\WINDOWS\TEMP (if it exists).
4. Install QuickTime using the version of the QuickTime you downloaded.
5. Restart Windows.

### Dashboard Issue Failure to Display Meetings That Have Started

In this release of Cisco Webex Meetings Server, the dashboard can fail to display certain meetings as having started. This issue occurs in the following scenario:

A meeting is scheduled with the **Allow participants to join teleconference before host** setting enabled. A participant joins the meeting by phone but does not join the web portion. The dashboard should indicate that this meeting has started and has one participant but it does not. This issue can cause users to schedule multiple meetings resulting in performance issues.

### Dial-in and Dial-Out Connections to an In-Progress Meeting

When a meeting fails over from one data center to another, the dial-in and dial-out connections to that meeting do not automatically reconnect. To reestablish the connections, participants hang up and manually dial back in.

This problem may occur when:

- The installed system is a large MDC.

- The meeting is started while one of the data centers is in Maintenance Mode or is powered down.
- When, after Maintenance Mode is turned off or the data center is powered on, another data center is powered off or placed into Maintenance Mode.

## IP Communicator 7.0.x Endpoints

IP Communicator 7.0.x endpoints joining CWMS meetings can introduce audio quality issues (echo and other noises) to a conference if either of the following conditions occur:

- IP Communicator is not muted.
- A participant using IP Communicator becomes the active speaker.

To prevent this issue, fine tune the IP Communicator environment (for example, the headset, microphone, and speaker) or use a different traditional phone.

## Keeping Your Hostname While Changing Your Virtual Machine IP Address

Never change the DNS entries for the hostnames that are configured in your deployment. You can change the hostname of a virtual machine that is part of your deployment. The corresponding IP address is picked up automatically from the DNS. To change the IP address of a virtual machine and keep the same hostname, perform the following steps:

1. Configure a temporary hostname in the DNS.
2. Change the hostname of the virtual machine to the temporary hostname that you configured.
3. Take the system out of maintenance mode for the new hostname change to take effect.  
Your original hostname is not part of the deployment after this change.
4. Change the IP address of the original hostname in the DNS to the new IP address.
5. Change the temporary hostname of the virtual machine to the original hostname.
6. Take the system out of maintenance mode for the hostname change to take effect.  
Now the original hostname is configured with your new IP address.

## Update from 3.0 Patch 1 Fails

Updating from Release 3.0 Patch 1 (3.0.1.33) fails because there is incorrect data in the cwms.pub file. Before you update from 3.0 Patch 1, apply the following workaround for this issue.

1. Go to <https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvj70890>.
2. Download the attached file: `fix_update.zip` and copy it to `/archive` directory on the primary Admin VM.
3. Use SSH to connect to the primary Admin VM, and navigate to the `/archive` directory.
4. Unzip the file: `unzip fix_update.zip`.
5. Make the unzipped file executable: `chmod +x fix_update`.
6. Run the executable: `./fix_update`.
7. After you see the `Success` message, proceed with the update.

## Caveats

We report open and resolved customer-found bugs of severity 1 to 3.

### Procedure

You can find details about listed bugs and search for other bugs by using the [Cisco Bug Search Tool](#).

**Note** For more info on using the Bug Search, see [Bug Search Tool Help](#).

### Closed Caveats in Cisco Webex Meetings Server Release 4.0MR4

The following caveats (bugs) are closed for this release.

Caveat ID Number	Severity	Description
<a href="#">CSCvx63985</a>	3	When a user joins a meeting from Android/IOS devices it automatically calls-in with the 2nd number
<a href="#">CSCvy31993</a>	3	Join meeting by URL as guest user failed
<a href="#">CSCvy10016</a>	3	PT:The exception mtg migrate failed if the migrate time is between exopt mtg start time and end time
<a href="#">CSCvx53272</a>	3	Migration: PT meeting migrated, while, invitee list is empty on cloud site
<a href="#">CSCvx18554</a>	3	Mobile alternate host/assistant cannot get host role in JBH mtg after others made too many attempts
<a href="#">CSCvw91725</a>	3	PT:Orion disable JBH-Presenter, the JBH attendee still can become presetner after migrated to train

### Open Caveats in Cisco Webex Meetings Server Release 4.0MR4

The following table lists caveats that are open in this release.

Caveat ID Number	Severity	Description
<a href="#">CSCvx65258</a>	3	video session terminated and cannot reconnect

### Resolved Caveats in Cisco Webex Meetings Server Release 4.0MR4

The following table lists caveats that were open in a previous release and that are fixed in this release.



Caveat ID Number	Severity	Description
<a href="#">CSCvv33371</a>	4	Catalina.out log doesn't rotate and affects collecting Infocap logs on Admin VM
<a href="#">CSCvv44797</a>	3	Include information in Planning Guide for CWMS that hyperthreading should be disabled
<a href="#">CSCvv57840</a>	3	CWMS Deprecate TLS 1.1 support
<a href="#">CSCvv81063</a>	3	CWMS admin guide - Grace host license description
<a href="#">CSCvw50598</a>	2	While joining meetings from Android devices users constantly have the audio option greyed out
<a href="#">CSCvw54945</a>	4	CWMS in weekly recurring meeting, editing days in week do not save for entire series in classic view
<a href="#">CSCvw92105</a>	3	Participants reports not detailed
<a href="#">CSCvx14698</a>	3	Guests are unable to join before hosts on recurring meetings
<a href="#">CSCvx28380</a>	5	The calculation of the "MP video" in the ParticipantReport.csv is incorrect
<a href="#">CSCvx43887</a>	2	jabber for iPhone cannot start CWMS meeting (iPhone Meet App can start meeting successfully)
<a href="#">CSCvx52215</a>	3	CWMS 4.0 MR3 SP4 - Wrong number displayed in Audio Connection dialog for Call-me
<a href="#">CSCvx58444</a>	3	computer audio disconnect after join meeting 10 mins for DDC
<a href="#">CSCvx67102</a>	6	Request for Icon Change for Buttons in 3.x Meeting Client Interface
<a href="#">CSCvx89772</a>	3	restful API - Scheduling more than 200 email addresses
<a href="#">CSCvx89774</a>	3	restful API - Adding participants in the scheduling meeting
<a href="#">CSCvx91059</a>	3	the meeting cannot start because there is no CB on MZM
<a href="#">CSCvy04383</a>	4	Participant privileges setting in private meeting room session not show text for remote control.
<a href="#">CSCvy11781</a>	3	CWMS sends duplicate emails to participants when one instance of a recurring meeting is edited
<a href="#">CSCvy27020</a>	3	Win Mac - Egypt outside Cairo should be Egypt in the Country/Region list on Audio Connection dialog
<a href="#">CSCvy28408</a>	3	CWMS supports macOS Big Sur
<a href="#">CSCvy29763</a>	3	No log info stored in to the conference_audit.log file causing rsyslog to not send conf info.

Caveat ID Number	Severity	Description
<a href="#">CSCvy29905</a>	3	Problem with the font on the Korean language

### Closed Caveats in Cisco Webex Meetings Server Release 4.0MR3

The following table lists caveats that are closed in this release.

*Table 2: Closed Caveats in Cisco Webex Meetings Server Release 4.0MR3 (Build 4.0.1.3237)*

Caveat ID Number	Severity	Description
<a href="#">CSCvi76477</a>	3	"<![CDATA" shows before the webex link when send invite using productivity tools

### Open Caveats in Cisco Webex Meetings Server Release 4.0MR3

The following table lists caveats that are open in this release.

*Table 3: Open Caveats in CiscoWebex Meetings Server Release 4.0MR3 (Build 4.0.1.3237)*

Caveat ID Number	Severity	Description
<a href="#">CSCvr96320</a>	3	Feature Send Email that Recording is ready to participants is broken

### Resolved Caveats in Cisco Webex Meetings Server Release 4.0MR3

The following table lists caveats (bugs) that were open in a previous release, and fixed for this release.

*Table 4: Resolved Caveats in CiscoWebex Meetings Server Release 4.0MR3 (Build 4.0.1.3237)*

Caveat ID Number	Severity	Description
<a href="#">CSCvi76477</a>	3	"<![CDATA" shows before the webex link when send invite using productivity tools
<a href="#">CSCvj83905</a>	4	Creating recurring meeting on user page creates 1 less entry on outlook
<a href="#">CSCvq07604</a>	3	FQDN of Admin VM present in Meeting Link
<a href="#">CSCvq66565</a>	3	Secure Call In to CWMS 4.0 may fail due to unsupported ciphers
<a href="#">CSCvq97578</a>	3	CWMS 4.0/Not able to search users while adding to a meeting in Modern View
<a href="#">CSCvr76722</a>	3	Users cannot hear and see each other in the meeting if using VoIP/Video - MMP issue

Caveat ID Number	Severity	Description
<a href="#">CSCvs08301</a>	2	Logs don't get archived daily on 4.0MR2 causing full fill of /triage partition
<a href="#">CSCvs15960</a>	3	Wrong timezone display for Brasilia & Fiji
<a href="#">CSCvs25223</a>	3	Issue with starting meeting from iPad on iOS ver.13
<a href="#">CSCvs32982</a>	3	When VM's time sync is back to normal, CWMS should send an email to Admin users
<a href="#">CSCvs36289</a>	2	Smart Software Licenses status Registration issue after successful register.
<a href="#">CSCvs43198</a>	3	CWMS System Expansion with Internal SSL SAN certificate changes documentation
<a href="#">CSCvs43377</a>	5	Missing information on cipher suites and malformed codec in documentation
<a href="#">CSCvs48929</a>	3	When the user has special characters in his name , it cannot be displayed when login to PT.
<a href="#">CSCvs63477</a>	4	audio only meeting keep too long
<a href="#">CSCvs66037</a>	5	After successful registration CWMS showing banner with the wrong type of licenses.
<a href="#">CSCvs91466</a>	3	Cisco Webex Meetings APP option "Don't show me these settings again" does not work as expected
<a href="#">CSCvs93244</a>	3	Users not able to download Desktop app in Modern View on large HA system
<a href="#">CSCvs95076</a>	3	Users are unable to log in via WebEx app from android/iOS and PC
<a href="#">CSCvt27399</a>	3	multimedia report showing empty
<a href="#">CSCvt31261</a>	3	If the primary CUCM is not reachable , Directory Integration button is not working properly.
<a href="#">CSCvt32840</a>	2	Video Minutes in the monthly report & meeting report showing incorrect value (0 minutes for video)
<a href="#">CSCvt55366</a>	4	CWMS skips input of Attendee ID when calling in

### Closed Caveats in Cisco Webex Meetings Server Release 4.0MR2

There are no closed caveats for Cisco Webex Meetings Server Release 4.0MR2 (4.0.1.2147).

### Open Caveats in Cisco Webex Meetings Server Release 4.0MR2

The following table lists caveats that are open in this release.

*Table 5: Open Caveats in Cisco Webex Meetings Server Release 4.0MR2 (Build 4.0.1.2147)*

Caveat ID Number	Severity	Description
<a href="#">CSCvq97578</a>	3	CWMS 4.0/Not able to search users while adding to a meeting in Modern View

## Resolved Caveats in Cisco Webex Meetings Server Release 4.0MR2

The following table lists caveats (bugs) that were open in a previous release, and fixed for this release.

*Table 6: Resolved Caveats in Cisco Webex Meetings Server Release 4.0MR2 (Build 4.0.1.2147)*

Caveat ID Number	Severity	Description
<a href="#">CSCvq80998</a>	3	Problem with login to the Cisco Webex Meeting App
<a href="#">CSCvq82613</a>	2	CWMS MDC Data center in blocked state after update to 4.0 from 3.0
<a href="#">CSCvr08883</a>	3	Garbled User Name in CWMS meeting client
<a href="#">CSCvr09779</a>	4	NFS storage mount procedure taking too long to reconnect storage causing various issues
<a href="#">CSCvr72540</a>	3	Smart Licensing page shows MDC usage in a single system
<a href="#">CSCvr79957</a>	3	Incorrect language of the user's website (only Moder View) of CWMS 4.0

## Open Caveats in Cisco Webex Meetings Server Release 4.0MR1

The following table lists caveats (bugs) that are open for this release.

*Table 7: Open Caveats for Cisco WebEx Meetings Server Release 4.0MR1 (Build 4.0.1.1110)*

Caveat ID	Severity	Headline
<a href="#">CSCvq57460</a>	3	Mac cannot start T32 client Orion MC/NBR meeting after started 39.5.6 client Orion MC/NBR meeting
<a href="#">CSCvq71488</a>	3	Win fail to install WDL (cannot share printable document) when start meeting from Jabber client

## Resolved Caveats in Cisco Webex Meetings Server Release 4.0MR1

The following table lists caveats (bugs) that were open in a previous release, and fixed for this release.

**Table 8: Resolved Caveats for Cisco WebEx Meetings Server Release 4.0MR1 (Build 4.0.1.1110)**

Caveat ID	Severity	Headline
<a href="#">CSCvp93853</a>	2	SL Conn Status showed Disconnected; resulted CWMS in eval mode when keepAlive mechanism failure
<a href="#">CSCvp58850</a>	3	Transport Gateway URL configuration error
<a href="#">CSCvq10811</a>	6	CUCM Cluster- AXL Failover Support

## Closed Caveats in Cisco Webex Meetings Server Release 4.0

The following table lists caveats (bugs) that are closed for this release.

**Table 9: Closed Caveats for Cisco WebEx Meetings Server Release 4.0 (Build 4.0.1.19)**

Caveat ID	Severity	Headline
<a href="#">CSCvp08700</a>	3	Win: Old PT can't update/delete meetings scheduled by new Webex App.
<a href="#">CSCvm99626</a>	4	Intermediate certificate lost after update to 2.8MR2 or 3.0MR2

## Open Caveats in Cisco Webex Meetings Server Release 4.0

The following table lists caveats (bugs) that are open for this release.

**Table 10: Open Caveats for Cisco WebEx Meetings Server Release 4.0 (Build 4.0.1.19)**

Caveat ID	Severity	Headline
<a href="#">CSCvp34644</a>	2	T39 Meeting crash when do sharing
<a href="#">CSCvp30778</a>	3	Desktop App failed to start the Webex meeting without any error message
<a href="#">CSCvo98359</a>	3	Old PT: Start instant meeting failed from old PT when login to 4.0 site.
<a href="#">CSCvp32096</a>	3	attendee cannot receive the recording ready mail

## Resolved Caveats in Cisco Webex Meetings Server Release 4.0

The following table lists caveats (bugs) that were open in a previous release, and fixed for this release.

**Table 11: Resolved Caveats for Cisco WebEx Meetings Server Release 4.0 (Build 4.0.1.19)**

Caveat ID	Severity	Headline
<a href="#">CSCvj02258</a>	3	Auto-upgrade to 3.0 fails from the system with HA
<a href="#">CSCvn47005</a>	3	The Calendar weekend days is Wrong
<a href="#">CSCvn67024</a>	3	Cannot login to PT when CUCM Publisher is down and Directory integration switched to CUCM Sub

Caveat ID	Severity	Headline
<a href="#">CSCvp16492</a>	3	When a call from SRTP endpoint is transferred to RTP endpoint there is no audio
<a href="#">CSCvo56983</a>	3	Users do not populate under search box from admin page nor from WHO field from web meeting setup
<a href="#">CSCvp03915</a>	3	SNMP USM User password cannot contain "\$" sign
<a href="#">CSCvn77979</a>	4	Force all users to change change password every XX day(s) option also affects LDAP users
<a href="#">CSCvo51406</a>	4	Call Me numbers are not showing in Edge Browser
<a href="#">CSCvo12211</a>	4	The Number of Participants in Meeting Search result does not show the exact values

## Additional Information and Service Requests

For information about submitting a service request, and for additional information, you can go to <http://www.cisco.com/c/en/us/support/index.html>.

You can also subscribe to Cisco Security RSS feeds and receive notifications when new information is available. Content feeds are available in both the 1.0 and 2.0 versions of the RSS format. Visit <http://tools.cisco.com/security/center/rss.x?i=44>.

---

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).

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: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. 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)

© 2019–2021 Cisco Systems, Inc. All rights reserved.