Release Notes for Cisco WebEx Meetings Server Release 2.7

First Published: 2016-11-29

Last Modified: 2018-07-13

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 2.7. 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.

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

Select **Products** > **Conferencing** > **Web Conferencing** > **WebEx Meetings Server** > **WebEx Meetings Server 2.7**.

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 2.7MR3

This section describes what is new for Cisco WebEx Meetings Server Release 2.7MR3.

Attention The 2.7MR3 software update is only for systems that are currently running Cisco WebEx Meetings Server Release 2.7.1.12, 2.7.1.1073, 2.7.1.2048, or later.

Invitation Email for an In-Progress WebEx Meeting

With this maintenance release and later, emails sent to invite or to remind people to join an in-progress meeting do not contain the calendar information.

Jabber Support

This maintenance release adds support for Cisco Jabber Release 11.8 and Release 11.9.

Meeting URL Security Patch

This patch (Build 2.7.1.2091) removes the **Eliminate unsecure data from URL links** option from the **Settings** > **Security** > **Short** link section of Site Administration. This option is permanently enabled to make meeting URLs more secure. This setting applies to all new meetings scheduled after the update.

For backwards compatibility, you can leave the **Block all long URL links** option unchecked. If you check this option to improve security, the long URLs for previously scheduled meetings become invalid.

Updated Browser Support

Windows:

- Internet Explorer: 11.0.9600.18738
- Chrome: 55–60
- Firefox: 51–55
- Edge (only for Windows 10): 40.15063.0.0

  With this maintenance release, the Edge browser is fully supported for starting meetings, but not for recording playback.

Mac:

- Safari: 10.1.2
- Chrome: 55–60
- Firefox: 51–55

WebEx Meeting Client Application

This release supports WebEx Meetings Application version 31.14.4.5 for Windows and Mac.

WebEx Network Recording Player

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

Windows: 31.14.4.5

Mac: 31.0.0.1100

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

This release supports WebEx Productivity Tools version 2.82.7000.1178 for Windows.

New and Changed Features for Cisco WebEx Meetings Server Release 2.7MR2

This section describes what is new for Cisco WebEx Meetings Server Release 2.7MR2.

Attention The 2.7MR2 software update is only for systems that are currently running Cisco WebEx Meetings Server Release 2.7.1.12 or 2.7.1.1073 or later.

Citrix XenApp Support

This release adds support for Citrix XenApp 7.6. Users can run the Meeting Client in XenApp application mode, with a supported browser.

The virtual operating system is the operating system delivered by the server. The host operating system is the operating system installed on the user's computer.

Table 1: Supported Virtual Operating Systems and Browsers

Operating Systems	Browsers
Microsoft Windows 2008R2 Server Windows 2012R2 Server	Internet Explorer 11.103.14393.0 Chrome 54.0.2840–54.0.2840.99 Firefox 49–50

Table 2: Supported Host Operating Systems and Browsers

Operating Systems	Browsers
Windows 7 (32-bit and 64-bit) Windows 8.1 (32-bit and 64-bit) Windows 10 (32-bit and 64-bit)	Internet Explorer 11.103.14393.0 Firefox 49–50 Chrome 54.0.2840–54.0.2840.99
Mac OS X 10.11 El Capitan Mac OS X 10.12 Sierra	Safari 10.0–10.0.1 Firefox 49–50 Chrome 54.0.2840–54.0.2840.99

There are known issues related to Citrix XenApp. For more information see Closed Caveats in Cisco WebEx Meetings Server Release 2.7MR2, on page 23.

Improved Meeting Join Experience

When an attendee enables the **Start my video in all meetings** setting, the video for their meetings starts when they choose their audio connection. This feature starts audio and video at the same time.

If the **Start my video in all meetings** setting is not enabled, and WebEx detects a camera, the attendee can do one of the following:

- To start video for the current meeting, select **Start My Video**.
- To start video for the current and all subsequent meetings, select **Start My Video in all Meetings**.

Problem Reports

Mac OS and Microsoft Windows users can generate problem reports from within a meeting by selecting **Help** > **Generate Problem Report**. Users can save the report locally as a .zip file, or send the file as an email attachment.

A problem report is a log file that you can use to make troubleshooting with Technical Support easier.

Updated Browser Support

This maintenance release adds support for the following browser versions:

Microsoft Windows

- Internet Explorer 11.103.14393.0
- Chrome 54.0.2840.99
- Firefox 50
- Edge (only for Windows 10) 38.14393.00

Mac

- Safari 10.0.1
- Chrome 54.0.2840.98
- Firefox 50

Updated Mac Operating System Support

This maintenance release adds support for MacOS 10.12.1, which is also known as Sierra.

WebEx Meeting Client Application

This maintenance release supports WebEx Meetings Application version 31.8.0.167 for Mac and Windows.

WebEx Network Recording Player

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

- **Windows:** 31.8.0.167
- **Mac:** 31.0.0.1100

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

This maintenance release supports WebEx Productivity Tools version 2.82.7000.1161 for Windows.

New and Changed Features for Cisco WebEx Meetings Server Release 2.7MR1

This section describes what is new for Cisco WebEx Meetings Server Release 2.7MR1.

Attention The 2.7MR1 software update is only for systems that are currently running Cisco WebEx Meetings Server Release 2.7.1.12.

End Meeting When Host and All Authenticated Participants Leave

This maintenance release introduces a new site administration option for meetings: **End meeting when host and all authenticated participants leave**. When this feature is not enabled, and the host selects **Leave meeting** without ending the meeting, host privileges pass to the next participant in the list.

Enable this option to limit host privileges to designated hosts and authenticated users, and to prevent inappropriate access to meetings. After you enable this option, the system chooses a new host from the participant list, in order of priority:

- Alternate host
- Authenticated presenter
- Authenticated attendee

The meeting ends when no authenticated participants remain.

Implementing this feature requires that you toggle Maintenance Mode on and off.

Jabber Support

This release adds support for Cisco Jabber 11.7.

Updated Browser Support

This maintenance release adds support for the following browser versions:

Windows:

- Internet Explorer 11.103.14393.0
- Chrome 53.0.2785.116m
- Firefox 48.0.2
- Edge (only for Windows 10) 38.14393.00

Attention The 64-bit versions of the FireFox and Edge browsers (on any Windows platform) are supported only for starting and joining meetings, by downloading the temporary application. For more information about the limitations for the Edge browser, see Windows 10 and Edge Browser Restrictions, on page 13.

Mac:

- Safari 9.1.3
- Chrome 53.0.2743.116
- Firefox 48.0.1

Updated Cisco Unified Communications Manager Support

This maintenance release adds support for Cisco Unified Communications Manager Release 11.5(1).

Updated Microsoft Windows 10 Support

This maintenance release adds support for Microsoft Windows 10 Redstone 1, also known as Windows 10 Anniversary Update (Version 1607).

WebEx Meeting Client Application

This maintenance release supports WebEx Meetings Application version 31.5.20.63 for Mac and Windows.

WebEx Network Recording Player

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

- **Windows:** 31.5.20.63
- **Mac:** 31.0.0.1100

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

This maintenance release supports WebEx Productivity Tools version 2.82.7000.1159 for Windows.

New and Changed Features for Cisco WebEx Meetings Server Release 2.7

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

For a complete list of system requirements, see the *Cisco WebEx Meetings Server Planning Guide and System Requirements Release 2.7*. Visit http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html.

All supported features from Cisco WebEx Meetings Server (CWMS) Release 2.6 (including features added in Maintenance Releases) are supported in CWMS 2.7. The data sheet for Cisco WebEx Meetings Server provides an overview of the features and benefits of CWMS. Visit http://www.cisco.com/en/us/prod/collateral/ps10352/ps10362/ps12732/data_sheet_c78-717754.html.

Change to Delivery Options

As of March 30, 2016, E-delivery is the only available delivery option for software ordered from the Product Update Tool (PUT).

Enforced Password Aging for Administrators

For sites that use single-sign-on (SSO) or LDAP authentication, password-aging settings apply to administrator passwords, which are used to sign into the Site Administration portal.

Enforced Numeric Password for Call-In Users

Site administrators can require the use of numeric passwords for call-in users. When enabled, this feature generates a random numeric password for call-in users joining a meeting that requires a password. The meeting invitation email includes the numeric password.

Enhanced Reporting

At the end of every month, WebEx automatically generates Meetings and Participants reports. Site administrators receive an email notification when the reports are ready.

Site administrators can download the reports in the following formats:

- Meetings Reports in a CSV file
- Participants Report in a CSV file
- Summary Report in a PDF file
- All three reports in a zip file

Jabber Support

This release introduces support for Cisco Jabber Release 11.6.

Meeting Recording Announcements

WebEx plays a message to inform call-in users that the meeting is being recorded when

- A call-in user joins an in-progress meeting that is being recorded.
- A call-in user is in a meeting and the host starts recording the meeting.

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.

Site administrators can create up to four custom session types. Once created, a session type cannot be deleted; but site administrators can modify or deactivate it.

Site administrators can use session types to make the following features available to users:

- Sharing options (application, desktop, web; and remote control for each of these options)
- Record meeting
- Video capability in meeting
- Audio capabilities (Call-In: On or Off, Call-Me: On or Off, Computer audio: On or Off) subject to the following limitations:
  - At least one of the three options must be enabled.
  - To disable Computer audio, enable Call-In.
  - To enable the Call-Me option, enable Call-In.

Note You can assign multiple session types to a host account. The available features for a particular meeting depend on the meeting type that the host selects, while scheduling the meeting.

System-Altering Operations

To perform one of the following system-altering operations, obtain the Release 2.7 Open Virtualization Archive (OVA) file.

- Expanding the system
- Adding High Availability
- Adding Internet Reverse Proxy (IRP)

Important Ordering any CWMS OVA media (full installation media) from the Product Update Tool (PUT), requires the submission of an A2Q form. The A2Q form is required to validate the system architecture.

TLS Support

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

This release supports Cisco Unified Communications Server Release 10.5.2 and later, up to 11.0.(1a), for secure teleconferencing.

User Email Address Update

Site administrators can change the email address for an individual user, or addresses for multiple users in bulk by using one of the following methods:

- The WebEx Administrator portal
- LDAP
- Identity Providers
- A CSV file (edited and imported)

Important If you plan to use this feature, there are required configuration changes to make and limitations to consider. For more information, see SSO and Email Address Changes, on page 13 and About SSO Configuration, on page 16.

Updated Browser Support

This release adds support for the following browser versions:

Windows:

- Internet Explorer 11.0.9600.18204

- Chrome 51.0.2704.79 m
- Firefox 47.0
- Edge (only for Windows 10) 25.105860.0.0

Attention The 64-bit versions of the FireFox and Edge browsers (on any Windows platform) are supported only for starting and joining meetings, by downloading the temporary application. For more information about the limitations for the Edge browser, see Windows 10 and Edge Browser Restrictions, on page 13.

Mac:

- Safari 9.1.1
- Chrome 51.0.2704.84
- Firefox 47.0

WebEx Meeting Client Application

This release supports WebEx Meetings Application version 31.4.0.41 for Windows and Mac.

WebEx Network Recording Player

This release supports the following Cisco Network Recording Player versions:

- **Windows:** 31.4.0.41
- **Mac:** 31.0.0.1100

WebEx Productivity Tools

This release supports WebEx Productivity Tools version 2.82.7000.1150 for Windows.

Supported Upgrade Paths

This release of Cisco WebEx Meetings Server supports upgrades from release 1.x to 2.7. The following points apply:

- An upgrade is defined as a replacement of the system to deploy major modifications that we made to the system.
- An update is defined as 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.
- When upgrading, you cannot skip a major version of the software and go directly to a companion maintenance release (MR).

  For example, to upgrade from 1.5MR5 to a 2.7MR, *upgrade* from 1.5MR5 to 2.7 and then *update* to the 2.7MR.

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

Caution Do not click **Restart** for one data center until the update for the other is complete, and both display the **Restart** button. When you update from Release 2.5MR6 or later to 2.7, restarting one data center before the update is complete for the other breaks replication.

Use the following table to determine your upgrade path to Cisco WebEx Meetings Server Release 2.7.

Installed Release	To Release	Path
1.0 to 1.1	2.8	**1.** Update to 1.5. **2.** Update to 1.5MR5 Patch 2 or later. **3.** Upgrade to 2.8.
1.5 to 1.5MR4	2.8	**1.** Update to 1.5MR5 Patch 2 or later. **2.** Upgrade to 2.8.
1.5 MR5	2.8	**1.** Update to 1.5MR5 Patch 2 or later. **2.** Upgrade to 2.8.
1.5 MR5 Patch 2 or later	2.8	Upgrade to 2.8.
2.0 to 2.0MR8	2.7	**1.** Update to 2.0MR9. **2.** Update to 2.7.
2.0MR9 or later	2.7	Update to 2.7.
2.5 to 2.5MR5	2.7	**1.** Update to 2.5MR6. **2.** Update to 2.7.
2.5MR6	2.7	Update to 2.7.
2.6 or any 2.6MR	2.7	Update to 2.7.
2.7 or any 2.7MR	Any 2.7MR	Update to the 2.7MR.

Important You cannot 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.

For more information, see the following documents:

- *Cisco WebEx Meetings Server Administration Guide Release 2.7*: http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html
- *Cisco WebEx Meetings Server Planning Guide and System Requirements Release 2.7*: http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html

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 *Administration Guide for Cisco WebEx Meetings Server Release 2.7*:

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.

Productivity Tools

EMC SourceOne

WebEx Productivity Tools does not support EMC SourceOne. Users of EMC SourceOne can experience performance issues.

Incompatible Versions

Each release of Cisco WebEx Meetings Server supports a specific version of the Cisco WebEx Productivity Tools client. Download the supported version of Productivity Tools from the Downloads link on your Cisco WebEx Meetings Server website. Using incompatible versions of these two applications can cause issues.

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. 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.

Sharing Limitations

When a presenter shares from a PC running Microsoft Windows 8 or Windows 10, attendees see gray boxes instead of the following WebEx components:

- WebEx session controls (a panel that appears at the top of the presenter's desktop when sharing in fullscreen mode)
- **Chat** window
- **Participants** window

If the presenter shares an application instead of their desktop, unshared applications or popups in the foreground appear as gray boxes to attendees.

Sharing and Dual Monitors

When some presenters share an application, attendees see areas of yellow mesh. This occurs if the presenter is using dual monitors and the primary monitor is smaller than the secondary monitor. The larger area of the secondary monitor appears as yellow mesh for attendees.

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 ablity 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 16.

Windows 10 and Edge Browser Restrictions

The following restrictions apply to Windows 10 and to the Edge browser and Cisco WebEx Meetings Server Release 2.7MR2 and earlier:

- The Edge and Mozilla Firefox 64-bit browsers are supported only for joining and starting meetings, using the WebEx Temporary Folder Solution (TFS). To start or join a meeting, participants must select **Run a temporary application to join this meeting immediately** each time.
- The temporary application filename consists of the encrypted WebEx Site URL, username, and client machine parameters. Therefore, some filenames are long. The Edge browser truncates long filenames during the file download. The temporary client application depends on the information in the filename; so if the filename is truncated, the temporary application cannot run.

Warning This limitation prevents users with Windows 10 and the Edge browser from joining some meetings on CWMS. The only workaround is to use a different browser to join the meeting.

- The Edge browser does not support the playback of WebEx recordings.

Note These restrictions do not apply to Cisco WebEx Meetings Server Release 2.7MR3 and later.

Virtual Desktop Infrastructure

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

- Citrix XenDesktop and XenApp are 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.

Important Notes

CWMS Licensing

Multi-data Center Licensing

Multi-data Center (MDC) licensing is required to join data centers to a system. Each data center requires an MDC system license; a MDC system requires a minimum of two licenses, one for each data center. A Single-data Center (SDC) does not require a system license. See "About MDC Licensing" in 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.

Host Licensing

The way Host (user) licenses are counted changed significantly in release 2.5. A user can host a maximum of two simultaneous meetings, consuming only one license. Previously, a user that hosted multiple meetings consumed multiple licenses. A Host licenses is not required to schedule or attend a meeting. See "License Status of Users" in 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.

Extended Capacity Licensing

The base deployment models are micro (50), small (250), medium (800) and large (2000). You can extend the capacity of a large deployment, from 2000 up to 4000 ports. You can reduce the capacity of an extended system deployment, down to the base large deployment of 2000 ports.

To extend or reduce the system capacity, you add or remove up to 3 extension units. Each extension unit adds up to 700 more ports, up to the maximum 4000 ports for the system. When you add 3 extension units, you double the system capacity by adding 700 + 700 + 600 ports.

To enable this feature, you require an Extended Capacity license.

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 5.0, 5.0 Update 1, 5.1, 5.5, or 6.0 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.

Support for 4096-bit Certificates

Cisco WebEx Meetings Server (CWMS) is hard-coded to use 2048-bit certificates for its SSL system certificate(s). Certificates can be either self-signed or signed by a private or public Certificate Authority (CA).

CWMS also supports the use of 4096-bit certificates when they are imported as

- a Secure Teleconferencing Certificate,
- an SMTP certificate,
- an SSO IdP certificate, or
- a part of an SSL system certificate bundle.

  Certificates imported as part of an SSL certificate bundle must be signed by a private or public CA.

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.

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_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_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)

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.

Productivity Tools Upgrade Notice

If a previously deployed Productivity Tools package has a different version or build number from a newly deployed Productivity Tools package and the upgrade is not blocked, your Productivity Tools client will notify you with an upgrade warning dialog box.

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.

Known Issues and Notices

Translated Documentation

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

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.

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.

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.

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.

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.

Meetings Started with iOS Devices

Meetings that are started with iOS devices cannot be recorded.

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.

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.

Caveats

Using the Bug Search Tool

Known problems (bugs) are graded according to severity level. These release notes contain descriptions of the following:

- Open customer-found bugs of severity 1 to 3
- Resolved customer-found bugs of severity 1 to 3
- Resolved Cisco-found bugs of significance

You can find details about listed bugs and search for other bugs by using the Cisco Bug Search Tool.

Before you begin

To access the Bug Search Tool, you need the following items:

- Internet connection
- Web browser
- Cisco.com username and password

Procedure

Step 1 To access the Bug Search Tool, go to https://tools.cisco.com/bugsearch/search.

Step 2 Sign in with your Cisco.com username and password.

Step 3 Enter the bug ID number in the “Search for” field, then press **Enter**.

Tip You can also navigate to a specific bug by entering https://tools.cisco.com/bugsearch/bug/<BUGID> where <BUGID> is the ID of the bug that you are searching for (for example, CSCab12345).

What to do next

For information about how to search for bugs, create saved searches, and create bug groups, select **Help** on the **Bug Search Tool** page.

Closed Caveats in Cisco WebEx Meetings Server Release 2.7MR3

There are no closed caveats for Cisco WebEx Meetings Server Release 2.7MR3 (Build 2.7.1.3047).

Open Caveats in Cisco WebEx Meetings Server Release 2.7MR3

There are no open caveats for Cisco WebEx Meetings Server Release 2.7MR3 (Build 2.7.1.3047).

Resolved Caveats in Cisco WebEx Meetings Server Release 2.7MR3

The following table lists the caveats (bugs) that are fixed in this release. Use the Bug Search Tool to find more information about a bug.

Table 3: Resolved Caveats in Cisco WebEx Meetings Server Release 2.7MR3 (Build 2.7.1.3047)

Caveat ID Number	Severity	Description
CSCvb99900	1	WebEx Productivity Tools World Writable
CSCvc39165	1	Cisco WebEx Meetings Server Directory Traversal Vulnerability
CSCvc88194	1	Cisco WebEx Browser Extension Remote Code Execution Vulnerability
CSCvd28091	1	JDK/JRE software needs to be upgraded to address several security vulnerabilities
CSCvd50728	1	Cisco WebEx Meetings Server Authentication Bypass Vulnerability
CSCve25950	1	Cisco WebEx Meetings Server Information Disclosure Vulnerability
CSCvc84858	2	Audio issues caused by lack of adequate security polices in selinux
CSCvc89943	2	SSLGW crashes on media VM and recovers resulting in DC going down for few minutes
CSCvd03369	2	Meeting fails to end due to DB exception
CSCvd65864	2	System fails to end meeting when DB holds data in replication leg during MDC replication
CSCve37565	2	Prompt delay of 30 seconds on DC system after restart one of media machines
CSCve72863	2	Memory leak on sslgw when accessing internal site

Caveat ID Number	Severity	Description
CSCvb67814	3	New delegate cannot edit single instance of old delegate recurring meeting
CSCvb78854	3	Joining audio using deprecated meeting number results in invalid meeting number
CSCvb79074	3	Browser freezes when many (more than 35 alternate hosts) are added to recurring meeting.
CSCvb96230	3	Delegation for PCN Meeting not working as per documentation/Design
CSCvc01124	3	Update from 2.6 to 2.7 failed because of rsa-cryptoj-6.1.3.2-13.x86_64 RPM
CSCvc01129	3	Update from 2.6 to 2.7 is stuck at postUpdate.sh script because of "find" procedure.
CSCvc03322	3	Custom Report Participant file shows users dialing into first access number which is wrong
CSCvc03356	3	Storage and Ports Test reports storage not reachable from IRP
CSCvc14829	3	Joining meetings via Edge browser using a temp client fails due to a long temp client file name
CSCvc26700	3	Core file shown up on sslgw-dmz after update from 27FCS on 27MR2 and turn off maintenance mode
CSCvc31861	3	After installing meeting client via MSI, still new files get created upon initial launch
CSCvc31886	3	DB mismatch from 2.6 to 2.7 due to session type feature leaves configuration unchangeable
CSCvc44204	3	db_set_cron_timing.sh causing slow reboot
CSCvc46118	3	Anyone can present in the meeting does not work when enabled
CSCvc46151	3	Dashboard updates not smooth, appears to be some period gap when there are no updates
CSCvc47765	3	Increase HSTS max age timer
CSCvc78296	3	CWMS PT showing in slow/decreased performance add-in list in outlook
CSCvc94595	3	Evaluation of Orion for OpenSSL Jan 2017
CSCvc96090	3	Evaluation of orion for OpenSSL Jan 2017
CSCvc96137	3	Outlook is slow to open a meeting that includes a CWMS meeting and a large number of invitees

Caveat ID Number	Severity	Description
CSCvc96249	3	IE 11 on Windows 10 cannot stream recordings properly
CSCvc97876	3	CWMS should reboot after changing Storage Server when taken out of Maintenance Mode
CSCvc98147	3	CWMS update fails if SELinux is disabled
CSCvd20436	3	DB Error: Please redeploy the virtual machine
CSCvd20975	3	Cannot join WebEx meeting as a Guest using Edge browser and temp meeting client
CSCvd41260	3	Previous alternate host removed from meeting on web using Save Only option still receives reminders
CSCvd90497	3	Status of a meeting in MeetingReport.csv is UNKOWN
CSCvd91949	3	Meeting Summary report is not received intermittently//2.7MR2
CSCve21068	3	Starting PT for the first time by using Outlook results in Dummy info in host's event
CSCve36029	3	Productivity Tools shows error when updating occurrence for a meeting series
CSCve37009	3	ELM page not accessible after update to 2.7 MR2 Patch5
CSCve39483	3	IRP sends intermediate certificate in incorrect order.
CSCve41156	3	CWMS client can't input 2 byte character directly on chat window
CSCve43701	3	Glitch page when space is at the beginning of email address during sign in
CSCve44877	3	CWMS Meeting Analyze gets Stuck
CSCve51377	3	Join before host is removed when meeting instance is changed.
CSCve56613	3	Alternate Host option missing on scheduling page
CSCve61559	3	Unable to delete meeting series with exceptions from Outlook/PT
CSCve76811	3	Not able to edit single occurrence of meeting multiple times. CWMS 2.7 MR2
CSCvf06936	3	CWMS T31 meeting client freeze wseclienttr.dll
CSCvf39886	3	No deletion in mdc_sessionhistory table when user login from web
CSCvf39892	3	Journal tables (%_J tables) are not deleted if DDCTS is missing

Closed Caveats in Cisco WebEx Meetings Server Release 2.7MR2

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

Table 4: Closed Caveats in Cisco WebEx Meetings Server Release 2.7MR2 (Build 2.7.1.2048)

Caveat ID Number	Severity	Description
CSCvc24099	3	Xenapp7.6: meeting crash if block access audio/video device
CSCvc24120	3	XenApp7.6: meeting crash (10%) once start via Mac access

Open Caveats in Cisco WebEx Meetings Server Release 2.7MR2

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

Table 5: Open Caveats in Cisco WebEx Meetings Server Release 2.7MR2 (Build 2.7.1.2048)

Caveat ID Number	Severity	Description
CSCvc03322	3	Custom Report Participant file shows users dialing into first access number which is wrong
CSCvb76762	3	Username is 0 for phone connected guest user in participant report
CSCvb78854	3	Joining audio using deprecated meeting number results in invalid meeting number
CSCvc01124	3	Update from 2.6 to 2.7 failed because of rsa-cryptoj-6.1.3.2-13.x86_64 RPM
CSCvc01129	3	Update from 2.6 to 2.7 is stuck at postUpdate.sh script because of “find” procedure.

Resolved Caveats in Cisco WebEx Meetings Server Release 2.7MR2

The following table lists the caveats (bugs) that are fixed in this release. Use the Bug Search Tool to find more information about a bug.

Table 6: Resolved Caveats in Cisco WebEx Meetings Server Release 2.7MR2 (Build 2.7.1.2048)

Caveat ID Number	Severity	Description
CSCvb59175	2	DB deadlocks result in negative meeting numbers
CSCvb48547	2	Evaluation of orion for Openssl September 2016
CSCvb48548	2	Evaluation of orion for Openssl September 2016
CSCvb86354	2	Early offer with SME not working
CSCvb50221	3	ParticipantReport.csv session type is blank

Caveat ID Number	Severity	Description
CSCvb87242	3	Email alerts not showing up in local language after 2.7 MR 1 update
CSCvb66100	3	Update timezone database according to new Turkey DST
CSCvb54326	3	Upload of SMTP SSL cert is failing to import cert into keystore
CSCvb02098	3	Memory allocation failure in SSLGW
CSCvb47815	3	Can not start meeting from Firefox 49.0.1
CSCvb85516	3	Evaluation of orion for CVE-2016-5195 (DIRTY CoW)
CSCvb69943	3	MDC External users fail to access meeting site when one datacenter is in maintenance mode.
CSCvc17588	3	Add HA with IRP failed with error platform 5

Closed Caveats in Cisco WebEx Meetings Server Release 2.7MR1

There are no closed caveats for Cisco WebEx Meetings Server Release 2.7MR1 (Build 2.7.1.1073).

Open Caveats in Cisco WebEx Meetings Server Release 2.7MR1

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

The build number format is X.X.Y.Z, where X.X is the release number, Y is the maintenance release, and Z is the hotfix number.

Table 7: Cisco WebEx Meetings Server Release 2.7MR1 (Build 2.7.1.1073)

Caveat ID Number	Severity	Description
CSCvb02098	3	Memory allocation failure in SSLGW
CSCvb47815	3	Can not start meeting from Firefox 49.0.1

Resolved Caveats in Cisco WebEx Meetings Server Release 2.7MR1

The following table lists the caveats (bugs) that are fixed in this release. Use the Bug Search Tool to find more information about a bug.

The build number format is X.X.Y.Z, where X.X is the release number, Y is the maintenance release, and Z is the hotfix number.

Table 8: Resolved Caveats in Cisco WebEx Meetings Server Release 2.7MR1 (Build 2.7.1.1073)

Caveat ID Number	Severity	Description
CSCva00792	2	CWMS doesn't end meetings that are joined via audio only

Caveat ID Number	Severity	Description
CSCva32093	2	Recording consolidation fails due to permissions on DCT file
CSCva33162	2	Cannot join WebEx meetings from the Android App
CSCva36624	2	Guest Cannot Join meeting via Mobile Device
CSCva44382	2	CWMS Update fails due to multiple client initiations
CSCva50466	2	Users cannot Join a meeting two minutes before the scheduled start time.
CSCva72619	2	WebEx productivity tool schedules wrong date on recurring meetings
CSCvb19442	2	MC crash after End Meeting
CSCuz74578	3	Meeting Summary Report still intermittently not sent out
CSCuz78537	3	CWMS Storage and Port testing check IRP connectivity on not-needed ports
CSCva03644	3	Duplicate entries for SystemMonInfo
CSCva07096	3	snmpd process sometimes fails on media nodes
CSCva18508	3	DB deadlocks on large system when large number of audio meetings end
CSCva21978	3	Need to reinstate DST for Egypt Time zone
CSCva26340	3	Customize report from dual data center are different (DC01 to DC02)
CSCva27868	3	PTools Requires Repeat Login When Firefox Proxy Settings Enabled
CSCva28165	3	Want to have all phones included into Participant reports
CSCva33481	3	PT alternate hosts window doesn't show all users
CSCva36418	3	“Join by number” doesn't work if JBH is not enabled
CSCva50280	3	Host cannot record in meet now meeting even when session type allows it
CSCva58279	3	cli monitor thread is stucked in “waiting” status
CSCva65829	3	Jabber invitees cannot join Meet Now meeting
CSCva67619	3	CUCM is checked from CWMS every hour when sync is disabled.
CSCvb05549	3	Ruby zombie processes on Sec admin VM causes slow CPU grow
CSCvb09710	3	Meeting client freezes with some webcams
CSCvb16697	3	Email notification is not sent immediately after scheduling a meeting

Caveat ID Number	Severity	Description
CSCvb16704	3	Delay observed when email notification need to be re-sent
CSCvb17723	3	Missing last occurrence from Recurrent Meeting
CSCvb34146	3	Monthly report is not generated for fresh deployed system on 2.7FCS
CSCvb38467	3	After update from 2.7FCS var/log/messages file is no longer populated

Closed Caveats in Cisco WebEx Meetings Server Release 2.7

There are no closed caveats for Cisco WebEx Meetings Server Release 2.7 (Build 2.7.1.12).

Open Caveats in Cisco WebEx Meetings Server Release 2.7

There are no open caveats for Cisco WebEx Meetings Server Release 2.7 (Build 2.7.1.12).

Resolved Caveats in Cisco WebEx Meetings Server Release 2.7

The following table lists caveats that were open in Cisco WebEx Meetings Server Release 2.6MR2, and resolved in this release.

Table 9: Resolved Caveats in Cisco WebEx Meetings Server Release 2.7 (Build 2.7.1.12)

ID	Severity	Description
CSCuy83254	2	CSV Injection in the Name Field
CSCuy83260	2	Email Address Update from User Profile
CSCuz27489	2	Orion 2.7 CVE-2013-1960 CVE-2013-1961 Heap-based buffer overflow
CSCuz52374	2	Evaluation of orion for OpenSSL May 2016
CSCuz52375	2	Evaluation of orion for OpenSSL May 2016
CSCuz52376	2	Evaluation of orion for OpenSSL May 2016
CSCuz59068	2	IRP sslgw fails when trying to close connection in certain situation
CSCuu40706	3	TLS 1.0 is flagged as Medium Vulnerability by PCI
CSCux00729	3	Evaluate CVE-2015-6360 for libsrtp Denial of Service (DoS)
CSCux31940	3	OpenSSL 0.9.8r CWMS vulnerabilities
CSCuz04914	3	Meetings not visible from Delegate user page when meeting time changed
CSCuz20976	3	SIP Report Information in CWMS MATS Report is empty
CSCuz27500	3	Orion 2.7 - CVE-2015-8126 Buffer overflow vulnerabilities
CSCuz39753	3	Full User synchronization is executed daily

ID	Severity	Description
CSCuz40244	3	Change of SM and Default GW of IRP VMs isn't propagated to Public VIP
CSCuz41836	3	ldap when clicking on save the settings disappear
CSCuz47250	3	Call-in numbers show not be in call-in numbers list in summary report
CSCuz48326	3	CWMS cyrilic character full name search fails
CSCuz56651	3	If PT does not load within 500ms Office 2013 the add-in will be disabled
CSCuz62956	3	Generating particular meeting log does nothing
CSCuz68974	3	Support for higher version of MS Edge browser for CWMS
CSCuz75899	3	Log file rotation needed for logs over 200MB
CSCuz78537	3	CWMS Storage and Port testing check IRP connectivity on not-needed ports
CSCuz81114	3	Particular Meeting log does not contain mats when email is sent

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.