Cisco Meeting Management

Cisco Meeting Management 1.0.1

(Build 1.0.1.51)

Release Notes

December 20, 2017

Contents

1 Introduction

Cisco Meeting Management is a management tool for Cisco's on-premises video conferencing platform, Cisco Meeting Server. It provides a user-friendly browser interface for you to monitor and manage meetings that are running on the Meeting Server.

Meeting Management interoperates with the following:

- Cisco Meeting Server 1000
- Cisco Meeting Server 2000
- Virtual Cisco Meeting Server
- Acano X-series: X2 and X3 servers

Meeting Management, with its current feature set, is included within existing Cisco Meeting Server licensing.

If you combine Meeting Management with Cisco TMS (TelePresence Management Suite), you can both schedule and manage meetings that are run on your Meeting Server Call Bridges.

1.1 The software

Meeting Management is a virtualized application that runs on a vSphere web client. Specifications of the VM (virtual machine) depend on how many simultaneous actions your Meeting Management has to perform or observe. See the specifications for our estimates on sizing related to the numbers of Call Bridges you are managing.

For security, there is no user access to the console after first run. Except for the installation process, all use of Meeting Management is via a browser interface.

1.2 Upgrading from previous version

Before you upgrade:

- Please make sure you have an up-to-date backup of your Meeting Management.

  See the Installation and Configuration Guide for instructions.
- Plan your upgrade so no important monitored meetings are taking place while you are performing the upgrade.
- Notify other users before you start upgrading.

> **Note:** All users, both video operators and administrators, will be signed out, and data for ongoing and recent meetings will be lost when you upgrade.

To upgrade Meeting Management:

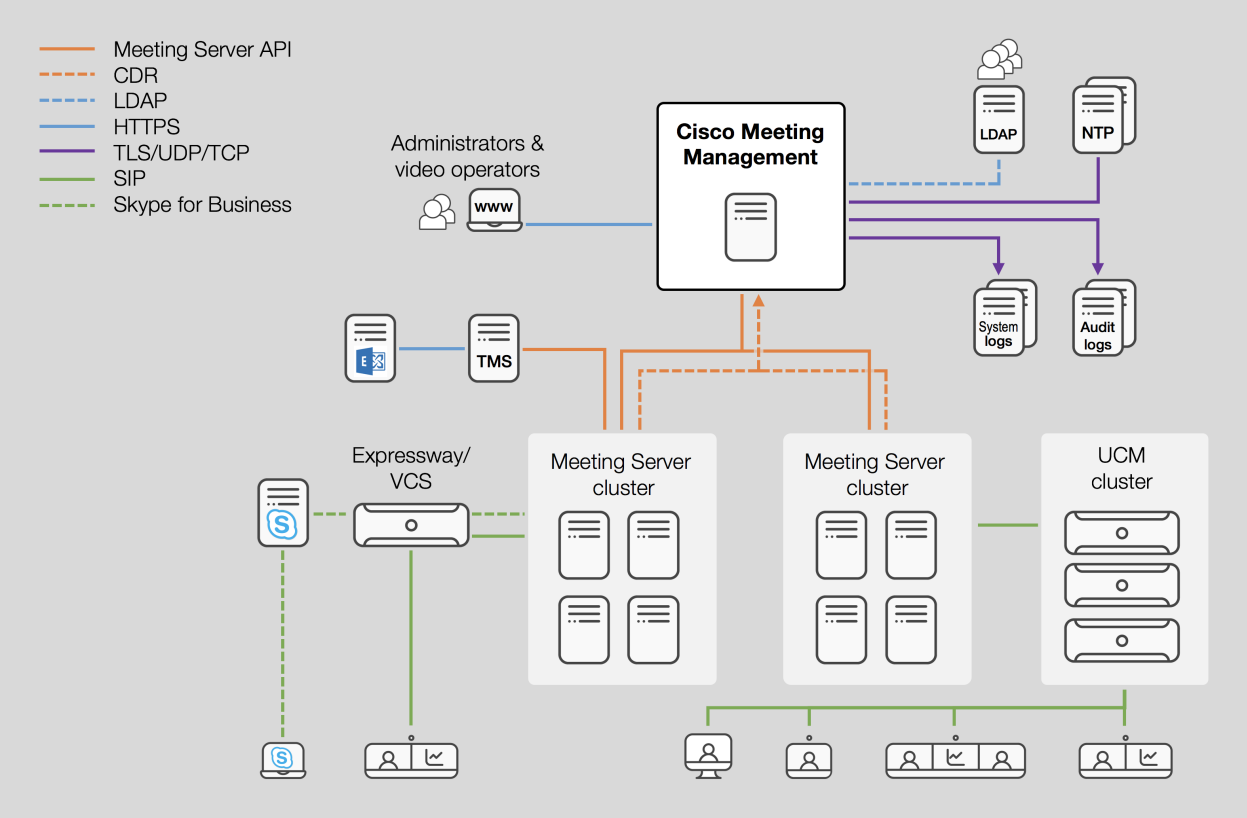
1. Sign in to the download area of cisco.com
2. Note the checksums for the new version of Meeting Management.
3. Download the upgrade image file and save it in a convenient location.
4. Sign in to Meeting Management.
5. Go to the **Settings** page, **Upgrade** tab.
6. Click **Upgrade**.
7. Click **Upload upgrade file**.
8. Select the upgrade image file and click **Open**.
9. Check that the checksums are the same as the ones displayed on the download site, then **Confirm**.

   If the checksums do not match, do not install the upgrade, as the file may have been corrupt.
10. **Restart** Meeting Management to complete the upgrade.

2 Deploying Meeting Management with the Meeting Server

One instance of Meeting Management can manage a small Meeting Server deployment with only a single Call Bridge or a large Meeting Server deployment with multiple clusters of Call Bridges as shown in Figure 1.

Figure 1: A single Meeting Management within a Meeting Server deployment



Meeting Management connects to Meeting Servers via the Call Bridge API. It installs itself as a CDR (Call Detail Record) receiver on each Call Bridge and gets information about active meetings via API requests and CDRs.

For greater reliability and accuracy you can configure more than one NTP server—Meeting Management supports up to 5 NTP servers. We recommend that Meeting Servers and instances of Meeting Management are connected to the same NTP servers.

Authentication of users

For user authentication, Meeting Management requires the use of an LDAP server.

Meeting Management differs from Meeting Server in that it does not import users, but instead maps to groups on the LDAP server and uses the LDAP server to authenticate users when they sign in and checks their group membership at that time. Make sure that you have configured appropriate user groups on your LDAP server before you set up Meeting Management.

Security and auditing

Meeting Management supports TLS 1.2 for its secure connections to its web interface and to connected servers. (Note that if a syslog server does not support TLS 1.2, then connections with TLS 1.1 or 1.0 will be made.)

Configuration backup files are with a user-supplied password.

Event logs for active meetings, as well as the latest system logs, are available in Meeting Management. Audit logs and system logs are sent to external syslog servers.

Diagnostics and troubleshooting

Meeting Management stores a limited amount of system logs locally. All audit and system logs can be sent to external servers.

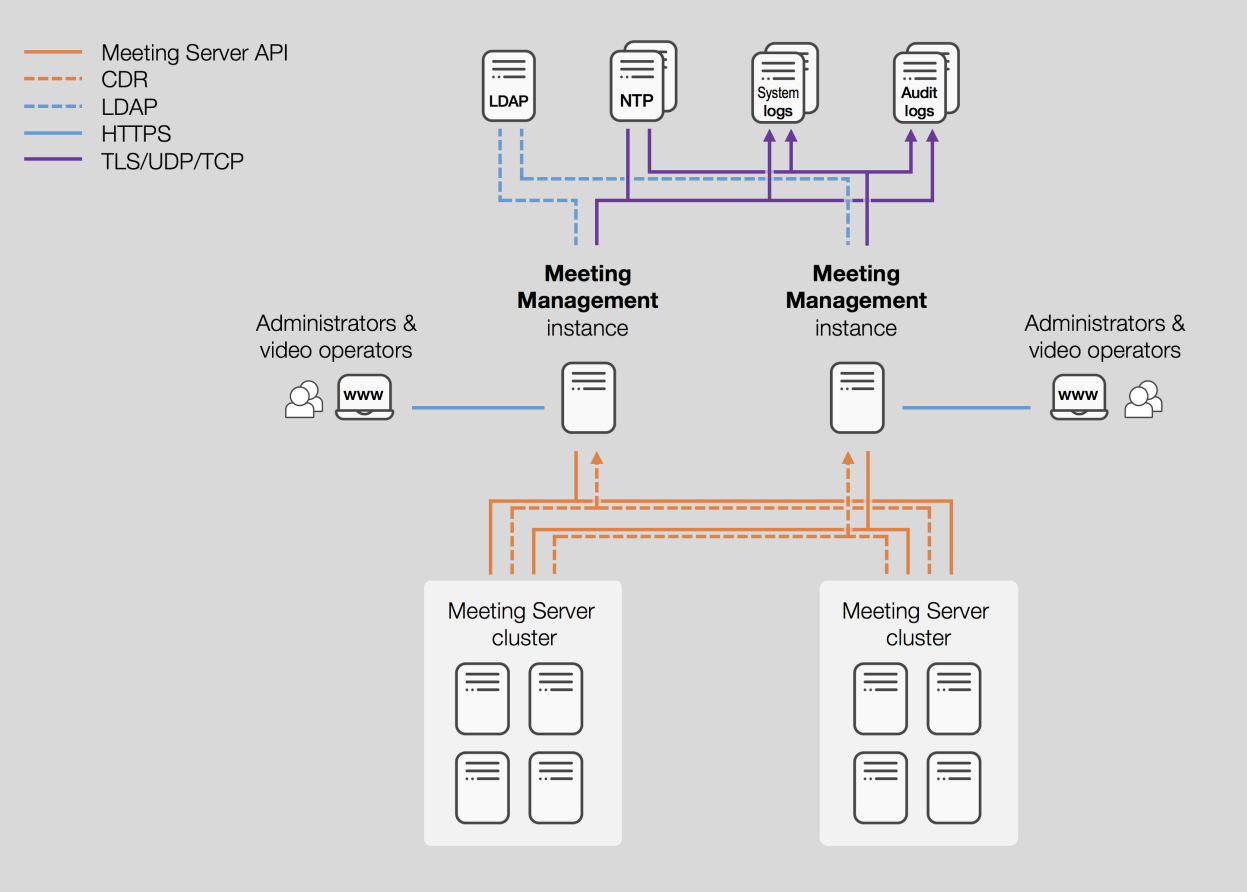
Crash logs and a log bundle are available for support purposes.

Call Bridge details or configuration details can be restored separately.

Resilience

To add resiliency to your Meeting Management deployment, you can connect up to 2 instances of Meeting Management to the same Meeting Server deployments. They must be configured independently—both get their information directly from the connected Call Bridges and no information is exchanged between them. We recommend that the 2 instances of Meeting Management are placed in different locations, see Figure 2.

Figure 2: A resilient Meeting Management deployment



2.1 Using with Cisco TelePresence Management Suite (TMS)

Cisco Meeting Management can work side by side with TMS, so you can use TMS scheduling features whilst using Meeting Management to monitor and manage your meetings.

TMS and Meeting Management work independently of each other, and Meeting Management gets its information directly from the Meeting Server. This means that you may see different details for scheduled meetings in TMS and Meeting Management.

For instance, a meeting scheduled in TMS is not displayed in Meeting Management before the meeting takes place. This is because the scheduling details are stored in TMS and never sent to the Meeting Server. The Meeting Server does not receive any meeting details until TMS starts a scheduled meeting by sending an API command, which is also when Meeting Management receives the information. And while TMS always displays the scheduled start and end time, Meeting Management always displays the actual start and end time for a meeting.

3 Specifications

3.1 Capacity

Meeting Management can manage anything from a single Call Bridge to multiple clustered deployments.

Specifications and requirements for two sizes of Meeting Server deployments are defined in the table below.

Note: If you have a medium size deployment and think you may need higher capacity later, then configure your VM for a large deployment.

	Small to medium deployments	Large deployments
Call Bridges	1-8 Cisco Meeting Server 1000 or 1 Cisco Meeting Server 2000 or 1-4 Acano X-series: X3 servers.	up to 24 Cisco Meeting Server 1000 or up to 3 Cisco Meeting Server 2000 or up to 10 Acano X-series: X3 servers
Call legs started at peak time	10 per second	20 per second
Users signed in to Meeting Management at the same time	15 users	25 users

4 Requirements and prerequisites

Before you get started with Meeting Management, check that your environment meets the requirements listed below.

For more information, see the Installation and Configuration Guide.

4.1 Minimum requirements for the Meeting Management VM

Requirement	Small and medium deployments	Large deployments
Server manufacturer	Any	Any
Processor type	Intel / AMD	Intel / AMD
Processor frequency	2.0 GHz	2.0 GHz
vCPU	4	8
Storage	100 GB, thick provisioned, eager zeroed	100 GB, thick provisioned, eager zeroed
RAM	4 GB	8 GB
Hypervisor	VMware ESXi 5.5 U2 or later, ESXi 6.0 U3, ESXi 6.5	VMware ESXi 5.5 U2 or later, ESXi 6.0 U3, ESXi 6.5
Network interfaces	1	1

For definitions of deployment sizes, see " Specifications" on page 9.

Note: If you have a medium size deployment and think you may need higher capacity later, then configure your VM for a large deployment.

4.2 Supported Cisco Meeting Server versions

Recommended	Minimum
2.2 or later	2.1.5 or later

Note: If participants join using access methods, we recommend using Meeting Server 2.2.8 or later to ensure that changing layout for the meeting affects all participants. For more information, see Meeting Server issue CSCvg01532.

Note: Owner for a meeting scheduled with TMS is only displayed if you use TMS 15.6 or later and Meeting Server 2.2.6 or later.

Note: 2.1.x versions do not support changing layouts for all participants in a meeting.

4.3 Call Bridge or cluster prerequisites

Before installing and configuring Meeting Management, ensure your deployment meets these prerequisites:

- **A user account on the Meeting Server API** . Meeting Management connects to Cisco Meeting Servers via the API. For security and auditing reasons, we recommend that you set up a separate account for Meeting Management.

  You need to use the same port as you would use to access the Web Admin Interface. For information on how to set up an account, see " Accessing the API" in the Cisco Meeting Server API Reference guide, found on the Programming Guides page on cisco.com.
- **CDR capacity.** Meeting Management configures itself as a CDR (Call Detail Records) receiver for each Call Bridge. Ensure the Call Bridge has suitable capacity for each instance of Meeting Management.
- **NTP server**. A time server must be configured for each Meeting Server in your deployment to make sure that Call Bridges and your Meeting Management are synchronized. We recommend using the same NTP servers for your Meeting Management and for your Meeting Server deployments. You may also require keys for your NTP server(s).
- **Recorder (Optional)**. If you want to use Meeting Management to start and stop recording, a Recorder must be configured on a Meeting Server within the deployment.
- **Streamer (Optional)**. If you want to use Meeting Management to start and stop streaming, a Streamer must be configured on a Meeting Server within the deployment.

4.4 Network requirements

For specific details on network requirements for installation, see the Installation and Configuration Guide.

4.5 Supported LDAP

All user access to Meeting Management is authenticated via an LDAP server when signing in. Users of Meeting Management must be members of one of the LDAP groups that Meeting Management has been told to use.

Supported LDAP implementations are:

- Microsoft Active Directory (AD)
- OpenLDAP

> **Note:** memberOf overlay must be enabled for OpenLDAP

Note: Meeting Management does not support nested groups. If a mapped group contains other groups, the members of those nested groups will not have access to Meeting Management.

Each user group can be assigned one of the following roles:

- **Administrators** have full access to Meeting Management. Administrators will typically set up Meeting Management, change configurations, add users, and monitor and maintain the system.
- **Video operators** only have access to the **Meetings** and **Overview** pages. Video operators monitor and manage meetings, and they perform basic troubleshooting related to ongoing meetings. For instance, they may try to call a participant who got disconnected or check the call statistics if someone has audio issues.

During the first time setup, you must add an administrator group that includes the person who will complete the initial configuration.

4.6 Supported browsers

Meeting Management is supported with the latest released versions of the following browsers:

- Microsoft Internet Explorer
- Google Chrome
- Mozilla Firefox
- Safari

> **Note:** Internet Explorer does not force updates, so we recommend that you manually check that you have the latest version.

> **Note:** Safari cannot be used for the first time setup because it does not work with a self-signed certificate. It may let you sign in with a self-signed certificate, but it will keep displaying the connection error window.

4.7 System log servers

Log storage has been restricted on Meeting Management, however, syslog records can be sent to a remote location. You can configure up to 5 external syslog servers to collect system logs.

We strongly recommend that you set up external syslog servers. Syslogs are required for troubleshooting and support.

4.8 Audit log servers

Audit logs are downloaded with the system logs and stored locally on Meeting Management, and they can be sent to a remote location as syslog records. You can configure up to 5 external syslog servers to collect audit logs.

Audit log servers are optional, but may be required in your organization.

The audit logs contain information on users' actions in Meeting Management, such as signing in, changing Meeting Management settings, or performing video operator actions.

Specific hardware or VM requirements for the syslog servers will depend on your Meeting Server deployment and your Meeting Management usage.

4.9 Certificate for Meeting Management

A self-signed certificate is created by Meeting Management during first time setup that Meeting Management will subsequently use with the browser interface, and when connecting to Call Bridges. However, this needs to be replaced by a CA (Certificate Authority) signed certificate. The certificate can be signed by an internal or external CA, depending on the requirements in your organization.

The CA signed certificates that can be uploaded to Meeting Management are:

- Meeting Management certificate to present to the web client and to Call Bridges.
- If using LDAPS, LDAP server certificate to add to Meeting Management's trust store.
- If using HTTPS verification, certificates for Call Bridges to add to Meeting Management's trust store.
- If using TLS, certificates for log servers to add to Meeting Management's trust store.

Note: The address used by Call Bridges as CDR receiver address can be the same address as your users use to access the browser interface. If you set up any alternative addresses, note that all addresses in use should be included in the certificate for Meeting Management. Additional addresses can be added in the SAN (Subject Alternative Name) field of the certificate.

4.10 Port information

Table 1: Ports for outgoing communication from Meeting Management

Purpose	Protocol	Destination Ports
Syslog	TCP/UDP	514 (or as configured)
Syslog	TLS	6514
LDAP	LDAP	389
LDAP	LDAPS	636
LDAP Global Catalog (where base DN is specified to DC level only)	LDAP	3268
LDAP Global Catalog (where base DN is specified to DC level only)	LDAPS	3269
Time synchronization (NTP)	UDP	123
Name resolution (DNS)	UDP	53
Meeting Server API	HTTPS	The TLS listening port for the webadmin as configured on the MMP of the Meeting Server

Table 2: Ports for incoming communication to Meeting Management

Purpose	Protocol	Destination Ports
Web interface and CDR receiver	HTTPS	443

Note: The administrator can configure Meeting Management-> Meeting Server connectivity on a port other than 443. If so, then the selected port will need to be opened in any firewall.

5 Overview of features

This first release of Meeting Management offers many features, comprising:

- Managing and monitoring meetings
- Security and auditing
- Account management and permissions
- Diagnostics and troubleshooting

The user interface provides:

5.1 NTP status

The NTP status shows Meeting Management's current time. It also shows for each configured and available NTP server the address, status, and offset between the NTP server and Meeting Management.

5.2 List of active or recent meetings

Meeting Management displays all active meetings and meetings that have ended within the last 30 minutes.

Note: If Meeting Management restarts, all meeting information is deleted. Only the list of active meetings is rebuilt after a restart.

In the meeting list view, you can see:

Meeting title	Name of space where the meeting takes place. If the meeting is not taking place in an existing space, the meeting title will be `call-<callCorrelator>`. The callCorrelator is an ID that is unique for the meeting.
Owner	If the meeting was scheduled using TMS 15.6 or above, the owner is the Scheduler specified in TMS. There is no owner specified if you scheduled the meeting using older versions of TMS. For all other meetings, an owner exists only if one has been specified on the Cisco Meeting Server. You can find more information, search for ownerName in the Cisco Meeting Server API Guide, and in the Cisco Meeting Server CDR Guide.
Current activity	Any streaming or recording taking place.
Participants	Number of connected participants in the meeting.

Start time	The time when the first participant joined.
Duration	Elapsed time for the meeting.
End time	The time the meeting ended. *Scheduled end times are not displayed.*

Note: If you are using TMS to schedule meetings, the start and end time in Meeting Management may differ from the scheduled time you see in TMS.

5.3 Pin meeting at the top of the list

You can pin important meetings at the top of the list—to do this, hover over the meeting in the list and click on the pin icon. A pinned meeting stays at the top until you unpin it, or until you sign out. To unpin a meeting, click on the pin icon on the left.

Note: You're automatically signed out 24 hours after you signed in.

5.4 Search by meeting title or owner, or by individual participant

A search field above the meeting list lets you search across both active and ended meetings for a meeting title or owner, or for an individual participant.

5.5 Meeting details

Select a meeting in the meeting list to see details. In the meeting details view you can:

- See the meeting title and meeting status details.
- Access meeting controls and event logs.
- See a list of meeting participants and filter by name or connection status.
- Add participants.
- Access participant details.

5.6 View and download event log for a meeting

Access event logs for the meeting using the meeting details view. Event logs provide the time stamp when somebody joined a meeting, left, started a recording, etc. Sort the logs by any column. Logs can be downloaded as .txt file.

Note: Timestamps on the **Meetings** page will use your local time zone (including the view of the meeting event log) based on your browser settings. The downloaded log will contain a UTC time stamp.

Note: All event logs are lost when you restart or upgrade your Meeting Management. Upon restart, partial logs will be recreated for meetings that are still ongoing, and for participants who joined the meeting and are still present, but their join time will appear to be the time of the restart.

Note: . All other log messages will be lost.

5.7 View a list of participants in a meeting

See a list of participants in the meeting filtered by:

- **All** - everyone who is in the meeting, is in the process of connecting, or has at any point been connected
- **Connected** - everyone who is currently in the meeting, or in the process of connecting
- **Disconnected** - everyone who has been in the call, but has been disconnected and has not been reconnected.

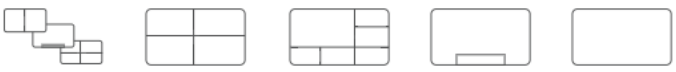
Note: For meetings in existing spaces: Although a meeting gets its title from the space where it takes place, Meeting Management only shows participants who joined this specific meeting.

In the list you can see:

Participant	Name of the participant
Start time	The time when the participant joined the meeting
End time	The time when the participant left the meeting
Actions	Call controls that let you control audio/video or drop the participant

5.8 Change layout for all participants in a meeting

You can change the video layout for all participants who are dialing in from a SIP endpoint. You can choose one of layouts shown here:



Changing the layout will only affect participants currently in the meeting and not participants who join after the change.

If they have permissions, individual participants can subsequently change the layout.

Note: Participants dialing in using Cisco Meeting App always have full control of their own layout. From Meeting Management you cannot see or control layouts for Meeting App participants.

Note: Only a subset of the existing Meeting Server layouts are available in Meeting Management.

5.9 Start and stop recording

If recording is configured on the Meeting Server, you can start recording a meeting, or you can stop an ongoing recording.

5.10 Start and stop streaming

If streaming is configured on the Meeting Server, and a streaming URI is set for the meeting you are managing, you can start or stop streaming.

5.11 Access controls and data about an individual participant

In the details for a meeting, select a participant's name to see detailed information. Here you can:

- See status details for the participant.
- Mute/unmute audio, stop/start video, or drop the participant from the meeting.
- See or change layout.
- See information about audio, video and presentation streams.

Note: Only SIP calls have all controls and call details available.

Note: For individual participants, you may see layout options that are not available for the endpoint in use.

Note: For some call types, such as Lync calls, no statistics are displayed.

Note: It may take up to 15 seconds before you can see if a participant has joined as an audio-only participant.

Note: If you search for an individual participant in the meetings overview, search results are listed by meeting title. That means that you cannot tell directly from the search results which meeting has the participant you are looking for.

Note: If you are viewing the participant side panel for a participant, you will not see the side panel updated when the participant rejoins the meeting. Closing and reopening the side panel will cause data to be displayed correctly.

5.12 View connected Meeting Servers

In the **Servers** view, you can see all servers, grouped in clusters. Unclustered servers are displayed as belonging to a single-node cluster.

5.13 Add and remove Call Bridge nodes or clusters

On the **Servers** page, you can add or remove Call Bridge nodes or Call Bridge clusters.

When you add a Call Bridge node belonging to a cluster, other Call Bridge nodes in the cluster are auto-discovered. They are displayed as ghost servers and listed as unmanaged servers until you add them. This saves you time when adding clusters.

5.14 Notifications

Get information about your system via notifications. On your **Overview** page, you can see the latest notifications listed, or you can click to see the full list.

5.15 Logs

Logs are useful for troubleshooting and auditing. In the current release, both system logs and audit logs are sent to your system log servers. Most recent entries are available on Meeting Management itself and can be downloaded via the Log bundle tab on the **Logs** page.

6 Bug search tool and resolved and open issues

You can now use the Cisco Bug Search Tool to find information on open and resolved issues for the Cisco Meeting Server, including descriptions of the problems and available workarounds. The identifiers listed in these release notes will take you directly to a description of each issue.

6.1 Using the bug search tool

1. Using a web browser, go to the Bug Search Tool. (https://bst.cloudapps.cisco.com/bugsearch/)
2. Sign in with a cisco.com registered username and password.

To look for information about a specific problem mentioned in this document:

1. Enter the bug identifier in the **Search** field and click **Search**.

To look for information when you do not know the identifier:

1. Type the product name in the **Search** field and click **Search**

   or,

   in the **Product** field select **Series/Model** and start typing `Cisco Meeting Management`, then in the **Releases** field select **Fixed in these Releases** and type the releases to search for example `1.0`.
2. From the list of bugs that appears, filter the list using the *Modified Date*, *Status*, *Severity*, *Rating* drop down lists.

The Bug Search Tool help pages have further information on using the Bug Search Tool.

6.2 Resolved Issues

6.2.1 Resolved in 1.0.1 (Build 1.0.1.51)

Reference	Issue
CSCvg37059	The initial install via the console does not allow you to configure a hostname which contains a period.
CSCvg50117	When adding a Meeting Server call bridge to Meeting Management, you cannot use a password that starts or ends with a space.

Reference	Issue
CSCvg56647	A vulnerability in the web interface of the Cisco Meeting Management could allow an unauthenticated remote attacker to affect the integrity of the device via a Clickjacking or Phishing attack. The vulnerability is due to the lack of proper input sanitization of iFrame data within the HTTP requests sent to the device. An attacker could exploit this vulnerability by sending crafted HTTP packets with malicious iFrame data. An exploit could allow the attacker to perform a Clickjacking or Phishing attack where the user is tricked into clicking on a malicious link. Protection mechanisms should be used to prevent against this type of attack.
CSCvg81542	Users attempting to log into Cisco Meeting Management with correct credentials may be presented with an error saying "Unable to contact server. Please try again." This can occur if either the "First Name" or "Last Name" attributes are in excess of 30 characters. For Unicode names (e.g. Cyrillic) this limit may be reached with as few as 7 visible symbols.

6.3 Open Issues

The following are known issues in this release. If you require more details on any of these please contact Support, https://www.cisco.com/support.

Reference	Issue
CSCvg44540	You cannot check which DNS server is being used by Meeting Management. This can be confusing if you have manually configured DNS servers and DNS servers are acquired via DHCP.
CSCvg44538	Configuration for the certificate and key for Meeting Management is on the **Settings** > **CDR** page. The heading for this page is misleading as the certificate and key are not related to CDR settings.

7 Interoperability

The interoperability test results for this product are posted to https://tp-tools-web01.cisco.com/start, where you can also find interoperability test results for Meeting Server.

7.1 Mute/unmute and layout behaviors

For more information on endpoint mute/unmute and layout control behaviors when used with Meeting Server and managed by Meeting Management, see:

- How will my endpoint mute/unmute controls behave when used with Cisco Meeting Server and managed by Cisco Meeting Management?
- How will my endpoint layout controls behave when used with Cisco Meeting Server and managed by Cisco Meeting Management?

8 Obtaining Documentation and Submitting a Service Request

Use the Cisco Notification Service to create customized flexible notification alerts to be sent to you via email or by RSS feed.

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

9 Product documentation

The following site contains documents covering installation, initial configuration, and operation of the product:

https://www.cisco.com/c/en/us/support/conferencing/meeting-management/tsd-products-support-series-home.html

9.1 Related documentation

Documentation for Cisco Meeting Server can be found at:

https://www.cisco.com/c/en/us/support/conferencing/meeting-server/tsd-products-support-series-home.html

Documentation for Cisco Meeting App can be found at:

https://www.cisco.com/c/en/us/support/conferencing/cisco-meeting-app/tsd-products-support-series-home.html

Document Revision History

Date	Description
2017-10-30	Original document published.
2017-12-07	ESXi 5.5 U2 or later has been added to supported hypervisors.
2017-12-20	Maintenance release 1.0.1 (Build 1.0.1.51)

Cisco Legal Information

Cisco Trademark