Cisco Meeting Management

Release 4.0

User Guide for Administrators

November 11, 2026

Contents

Document revision history 7

1 Introduction 8
- 1.1 What is new in 4.0 8
- 1.2 The software 9

2 Deployment overview 10
- 2.1 Authentication of users 11
- 2.2 Security and auditing 11
- 2.3 Diagnostics and troubleshooting 11
- 2.4 Integration with Cisco TelePresence Management Suite (TMS) 12
- 2.5 Licensing of the Meeting Server 12
- 2.6 Connection to the Cisco Smart Software Manager for Smart Licensing 12
- 2.7 Cisco Meeting Server Cloud Connector for email or Webex Teams notifications 13
- 2.8 Provisioning users and creating space templates on Meeting Server clusters 13
- 2.9 Resilience 13
- 2.10 Capacity limitations if you have large volumes of meetings 14
- 2.11 If you are using the Cisco Meeting Server API or 3rd party tools 14

3 Overview - view notifications, Cloud Connector status, and license status 15

4 Meetings - monitor and manage meetings 16

5 Spaces - Space management and blast dial configuration 17
- 5.1 Space management 17
  - 5.1.1 Creating spaces 17
  - 5.1.2 Viewing spaces 18
  - 5.1.3 Editing spaces 18
  - 5.1.4 Deleting spaces 19
  - 5.1.5 Join information 19
  - 5.1.6 Edit access role 19
- 5.2 Blast dial configuration 19
  - 5.2.1 Configurations 20
  - 5.2.2 Adding dial-out contacts 20

6 Users - Add users or edit user settings 22
- 6.1 About users 22

6.2 Edit LDAP server details 24
6.3 Assigning spaces to video operators 24
6.4 Add LDAP groups 25
6.4.1 Add LDAP user groups 25
6.5 Set up security policies for local users 26
6.6 Add local users 29

7 Servers – add or edit Servers 31
7.1 Add Configured Server 31
7.2 Configure New Server 35
7.2.1 Staging 35
7.2.2 Adding a new Meeting Server 35

8 Certificate 39
8.1 CA Signed Certificate 39
8.1.1 New certificate via CSR 39
8.1.2 Use Existing Certificate and Key 41
8.2 Self Signed Certificate 42

9 Network 43
9.1 Deleting a DNS or NTP server 43

10 Call Bridge 45

11 Web Bridge 46

12 Conferencing User 47
12.1 Customizing the LDAP Search and user mappings 49

13 Security 52

14 Push Configuration 53
14.1 SSH capability 53

15 Disable meeting management for a cluster 54

16 Provisioning 55
16.1 What is a space? 55
16.2 What is a space template? 55
16.3 Provisioning steps 55
16.4 Provisioning – Before you start 56

16.4.1 Supported LDAP implementations 56
16.4.2 LDAP server details 57
16.4.3 User import details 57
16.5 Provisioning – LDAP servers 58
16.5.1 How to add an LDAP server 58
16.6 Provisioning – Import users 59
16.6.1 How to add a user import 59
16.7 Provisioning – Automatically create spaces 61
16.7.1 Add rules for automatically creating spaces 61
16.8 Provisioning – Allow users to create spaces 65
16.8.1 Limitations 65
16.8.2 How to assign space templates to specific web app users 66
16.9 Provisioning – Review and commit 69
16.10 Provisioning – LDAP sync 70

17 Logs – logs, crash reports, detailed tracing 71
17.1 Meeting Management logs 71
17.1.1 Log bundle 71
17.1.2 System log servers 71
17.1.3 Audit log servers 72
17.1.4 Crash reports 72
17.1.5 Detailed tracing 73
17.1.6 90 day license report 73
17.2 Capture PCAP files in Meeting Management 73
17.3 Meeting Server logs 74
17.3.1 Log bundle 74
17.3.2 Detailed tracing 74
17.4 Add or edit log servers 75

18 Licenses 78

19 License status and enforcement 80
19.1 Available trials 81
19.2 License status during and after trial 83
19.3 Enforcement and warnings 83

20 Blast dial monitoring 85

21 Settings – configure Meeting Management 86

21.1 Edit network details 86
21.2 Upload certificate 87
21.3 Edit CDR receiver address 87
21.4 Connect to TMS 88
21.4.1 Associate cluster with TMS 89
21.4.2 Get access to TMS phonebooks 89
21.5 See NTP status or add NTP servers 90
21.6 Add SMTP Servers 91
21.7 Licensing 93
21.7.1 How to enable Smart Licensing 94
21.7.2 Smart Licensing actions after Smart Licensing has been enabled 96
21.7.3 License Reservation 96
21.7.3.1 License Reservation 97
21.7.3.2 Update reserved licenses 100
21.7.3.3 Returning reserved licenses 102
21.7.3.4 Things to consider while migrating to Smart license 103
21.8 Cisco Meeting Server Cloud Connector 104
21.8.1 Cisco Meeting Server Cloud Connector status 104
21.9 Display messages when users sign in 104
21.10 Configure advanced security settings 106
21.10.1 Rate limit sign-in attempts 106
21.10.2 Idle session timeout 107
21.10.3 Reset meeting server password 107
21.10.4 TLS settings 107
21.11 Backup and restore 108
21.11.1 Create a backup 108
21.11.2 Restore a backup 109
21.12 Upload keys to validate upgrade images 110
21.13 Restart Meeting Management 111

Appendix A Security hardening 112

Accessibility Notice 113

B Accessibility support features 114
B.1 Keyboard navigation 114
B.2 Screen reader support 114

Cisco Legal Information 115
Cisco Trademark 116

Document revision history

Table 1: Document revision history

Date	Description
2026-11-11	Document published

1 Introduction

This guide is for administrators of Cisco Meeting Management.

Cisco Meeting Management is a management tool for Cisco's on-premises video conferencing platform, Cisco Meeting Server. It manages licensing and provides a user-friendly interface to the Meeting Server.

As a Meeting Management administrator, you can:

- Install and configure Meeting Management
- Edit licensing settings for the Meeting Server
- Provision space templates and web app users on the Meeting Server
- Act as a video operator

A video operator can:

- View all active meetings and meetings that have ended within the last week
- View upcoming meetings that have been scheduled using Cisco TMS (TelePresence Management Suite)
- Manage active meetings
- See current Meeting Server license status

Cisco Meeting Management 3.0 or later is mandatory with the Meeting Server 3.0 or later, and it requires no additional licensing.

1.1 What is new in 4.0

For a general overview of new features and changes, see the release notes.

We have added the following sections in this release:

- Add SMTP Servers: We have added the procedure to configure an email address to receive alerts when license usage limit exceeds or when the system falls out of licensing compliance.

We have updated the following sections in this release:

- Licensing: We have updated the note in License reservation section mentioning encryption license is highly recommended for all customers to enable encryption on Meeting Server call bridges

1.2 The software

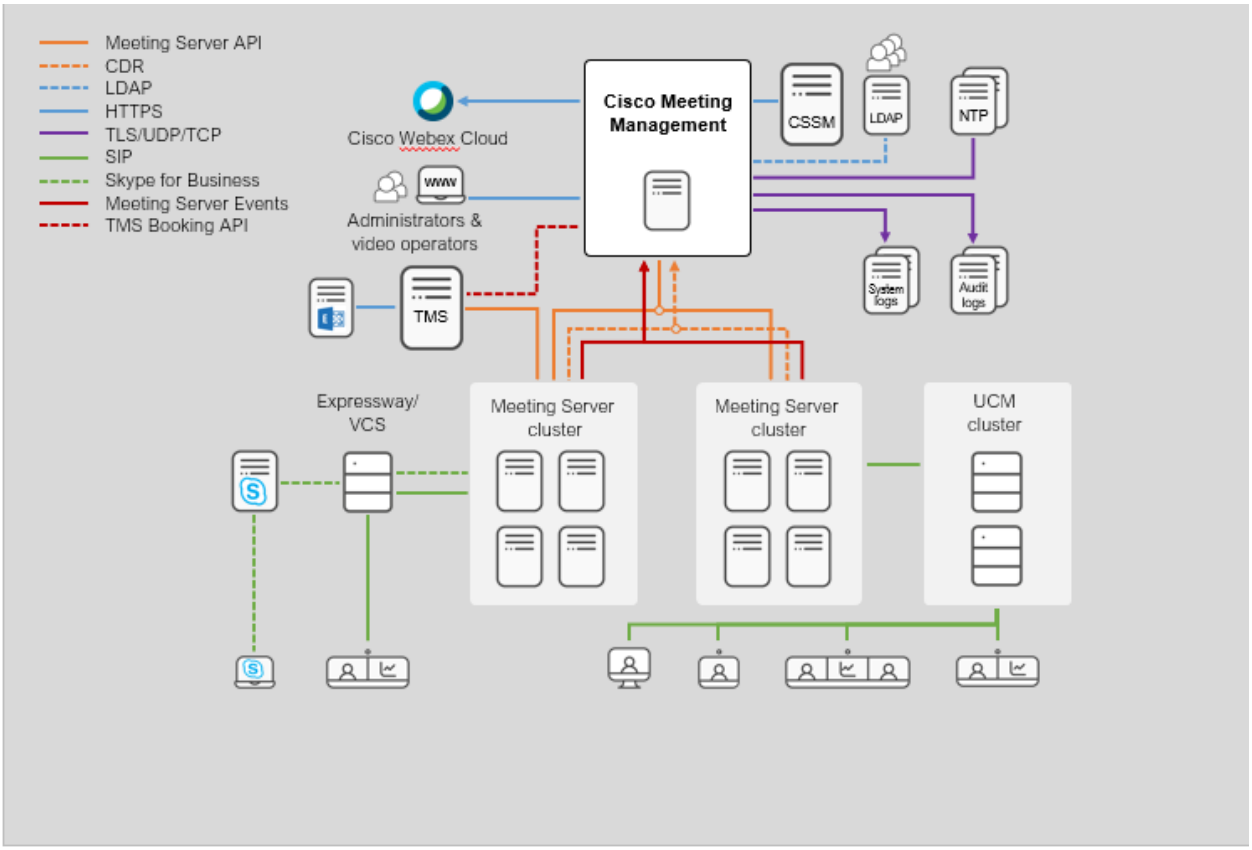
Meeting Management is a virtualized appliance. Specifications of the VM (virtual machine) depend on how many simultaneous actions your Meeting Management has to perform or observe. See the *Installation and Configuration Guide* for specifications and requirements, including our estimates on sizing related to the number of Call Bridges you are managing.

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

2 Deployment overview

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 below.

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



Meeting Management connects to Meeting Servers via the Call Bridge API. To get information on meeting activity, it installs itself as a CDR (Call Detail Record) receiver and events client on each Call Bridge and gets information about active meetings via API requests, CDRs, and Meeting Server events.

Note: If you choose to only use Meeting Management for licensing and provisioning for a cluster, then Meeting Management will not act as a CDR receiver or events client for Call Bridges in that cluster.

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

2.1 Authentication of users

Meeting Management supports locally managed users as well as user authentication via LDAP. You can choose to have only local users, only LDAP users, or both.

- **Local users** are added and managed locally on the Meeting Management **Users** page. These users are authenticated directly by Meeting Management.

  One local administrator user is generated during installation, and you can add more users after you have signed in for the first time. Local users are useful for setup and test, and for making LDAP changes without getting locked out of Meeting Management.

- **LDAP users** are added via mappings to existing groups on your LDAP server. Meeting Management uses your LDAP server to authenticate these users by checking their group membership when they sign in.

  Authentication via LDAP is recommended for general use and administration.

We recommend that you maintain at least one local administrator user account. This ensures continued access to Meeting Management in the event of LDAP issues. For general production use, we recommend that users are authenticated via LDAP. If authentication issues occur, LDAP users can reset their passwords on the LDAP server and then log in to Meeting Management again. Local users can reset their credentials with the assistance of other administrators. If the local administrator encounters authentication issues and they are the only administrator account available, the password cannot be recovered. In such cases, the local administrator user must re-install Meeting Management after removing all the existing data.

Note: All users can be either administrators or video operators. Their permissions depend only on the role, not whether they are managed locally or via LDAP.

2.2 Security and auditing

Meeting Management supports TLS 1.2 for its secure connections to its web interface and to connected servers.

Backup files are protected with a user-supplied password.

Event logs for active and recent meetings are available in Meeting Management. Audit logs and system logs can be sent to external syslog servers.

Also, advanced security settings let you comply with your organization's security policies if specific settings are required.

2.3 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, local user accounts, and passphrase dictionary can be restored separately from other configuration details.

2.4 Integration with Cisco TelePresence Management Suite (TMS)

Cisco Meeting Management can be integrated with TMS, so you can use TMS scheduling, endpoint management, and phone book features while using Meeting Management to monitor and manage your meetings.

Meeting Management connects to TMS via its booking API, and every 5 minutes it checks that it can access phone books and updates information about scheduled meetings. Upcoming meetings are seen in Meeting Management up to 24 hours before their scheduled start time.

For a more seamless management across Meeting Management and TMS, each scheduled meeting has a direct link from its meeting details in Meeting Management to its editing page in TMS.

2.5 Licensing of the Meeting Server

Meeting Management is mandatory with Meeting Server 3.0 or later for licensing purposes. If you are using Smart Licensing, then you must connect to the Cisco Smart Software Manager. Meeting Management has deprecated the support for local license files (traditional licensing mode) and has introduced license reservation. In an environment where Meeting Management cannot connect to the Internet due to security reasons, License reservation can be used to activate features and reserve licenses. For more information see Licensing section.

Note: Cisco Smart Licensing Portal Root CA will be updated in February 2023. If you are using Smart Licensing (online, SLR or PLR), it is recommended to upgrade to 3.6 or above while adding new licenses, adding a call bridge or performing a manual sync.

2.6 Connection to the Cisco Smart Software Manager for Smart Licensing

You can use Meeting Management to monitor whether your Cisco Meeting Server deployments are using more licenses than you purchased.

Meeting Management uses the Smart Agent to communicate with the Cisco Smart Software Manager (Cisco SSM). Meeting Management sends daily usage reports to Cisco SSM, and Cisco SSM then reports back whether the deployment is in compliance.

Note: If you have more than one instance of Meeting Management connected to the same Meeting Server cluster, for example to add resilience, then only one instance of Meeting Management should be connected to the Cisco Smart Software Manager. If you connect both instances, the reported usage will be counted twice.

2.7 Cisco Meeting Server Cloud Connector for email or Webex Teams notifications

You can connect to the Webex Control Hub to see status for Meeting Management deployments from the Webex Control Hub interface and set up email or Webex Teams alerts.

The Cloud Connector also sends statistics to Cisco so we can improve our products. If you want to see what information is sent, see the Cisco Meeting Server Cloud Connector online help.

2.8 Provisioning users and creating space templates on Meeting Server clusters

You can use Meeting Management to provision Cisco Meeting Server web appusers by importing users from one or more LDAP servers to connected Meeting Server clusters. You can also create space templates, which are pre-configured space settings that web app users can use to create new spaces.

Note that Meeting Management is not communicating directly with the LDAP servers for this purpose. Instead, LDAP server details and filter settings are sent to the Meeting Server, and the Meeting Server uses the details to provision users when an LDAP sync is triggered.

Note: For security and auditing reasons, we recommend that you create a separate bind user account for each Meeting Server cluster on each LDAP server.

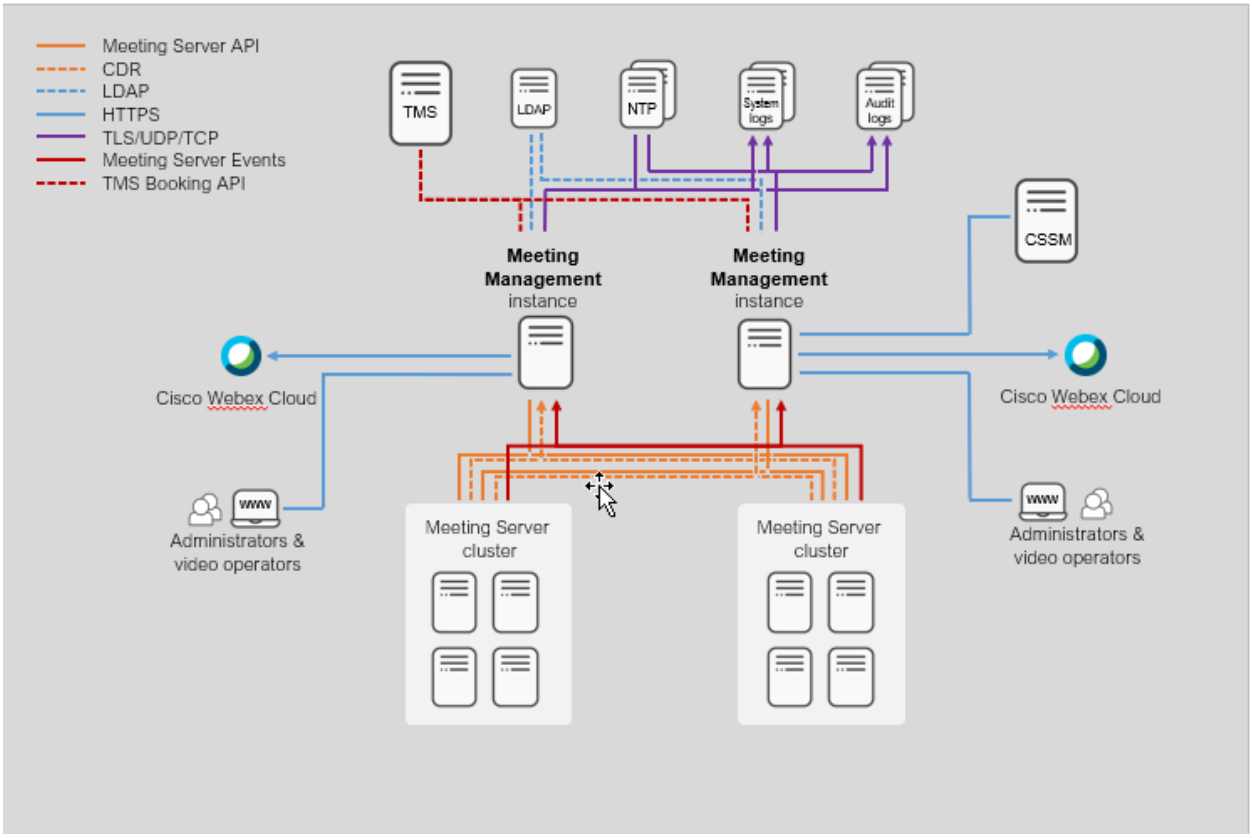
2.9 Resilience

To add resilience to your Meeting Management deployment, you can connect up to two 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 TMS servers. No information is exchanged between them. We recommend that the two instances of Meeting Management are placed in different locations so e.g. power outages or connection issues will not affect both instances at once.

There is no failover; both instances are active at all times, and settings that are local to Meeting Management, such as pinning a meeting at the top of the list, are only seen in the instance of Meeting Management where they were set.

Note: For resilient deployments, use only one instance of Meeting Management for licensing to avoid duplicate reporting. See Licensing.

Figure 2: A resilient Meeting Management deployment



2.10 Capacity limitations if you have large volumes of meetings

The performance of the meeting management functionality depends on the volume of meetings on the connected Call Bridges. See the capacity table in the "Before you start" section of the *Installation and Configuration Guide* for capacity limitations. If you have a deployment that exceeds the capacity for large deployments, then you must disable the meeting management functionality. You can do this individually for each connected cluster.

2.11 If you are using the Cisco Meeting Server API or 3rd party tools

We strongly recommend that you do not use the API – or any 3rd party tool using the API – to manage active meetings at the same time as you monitor or manage meetings using Meeting Management.

3 Overview – view notifications, Cloud Connector status, and license status

On the **Overview** page you can always see system notifications and Webex Edge status.

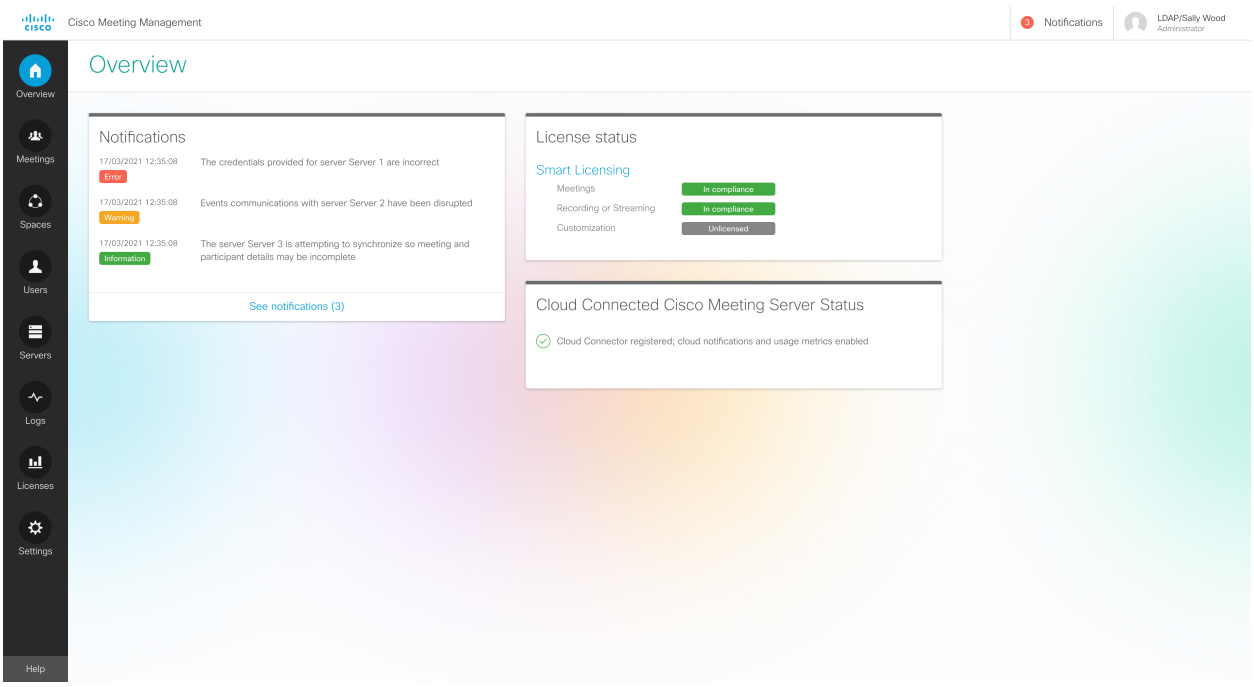
Notifications are always visible on the **Overview** page, and a counter in the top bar tells you if there are any current notifications.

Notifications have 3 levels of severity:

- **Error**: Critical issue
- **Warning**: Issue that you must act on to keep Meeting Management running
- **Information**: Useful information or minor issue

If licensing is enabled on the instance of Meeting Management you are signed in to, you will also see license status for the Cisco Meeting Servers.

If Meeting Management is using Smart Licensing, then the license status is the same across all connected clusters. When you click on the blue **Smart Licensing** heading you will be taken to the **Licenses** page where you can see and edit details.



Note: The number of notifications in the top bar is updated every 30 seconds, so it may temporarily differ from the number seen on the **Overview** page.

4 Meetings - monitor and manage meetings

On the **Meetings** page, you can act as a video operator to monitor and manage meetings. For instructions, see the *User Guide for Video Operators*, the online help, and our knowledge base articles.

5 Spaces - Space management and blast dial configuration

Meeting Management supports creating spaces and configuring blast dial, to quickly hold a meeting with a group of users.

You can add a predetermined list of participants to a space where you configure blast dial. When any participant dials in to the space, all the other participants are dialed out simultaneously.

Participants can press the DTMF digit **1** to enter the meeting and ***** to reject the call. When the participants press ***** and reject the call Meeting Management stops re-dailing the participants. Participants can also reject a call by pressing **Decline** or **Reject** buttons.

Note: Any other DTMF digits will be ignored and Meeting Management will continue to re-dial the participant until they press **1** or *****.

5.1 Space management

Meeting Management allows administrators to create and manage spaces. You can create, view, edit, and delete spaces on Meeting Server cluster and configure blast dial.

Video operators can also create and edit spaces using Meeting Management and assign tags to those spaces. These tags can be assigned to video operators, giving them access to specific spaces and the meetings associated with those spaces only.

5.1.1 Creating spaces

Follow these steps to create a space in Meeting Management:

1. On the **Spaces** page, click **Create space** button to launch **Create a Space** pop-up window.
2. Select the Meeting Server cluster from the drop-down menu.
3. Enter a unique name for the space in **Space name**, with a maximum character limit of 200.
4. Select the space tag from the **Space tag** drop-down. The drop-down lists all the tags that are assigned to the video operator.

   Note: The **Space tag** drop-down is only available for video operators and administrators cannot see it.

5. Select appropriate space template from **Templates**. If the templates are not available, it has to be created from the Meeting Server.
6. Click the **Create** button.

The created space will be listed in the **Spaces** page. Spaces with ongoing or active meetings will be displayed with  icon. Here, the number on the icon represents the total participants attending the meeting. Hovering over the icon displays a message, in this case, **Active meeting with 4 participants**.

5.1.2 Viewing spaces

You can view all the spaces in your cluster. Use the search bar to filter out the space you are looking for. Clicking on the space name takes you to the **Join Information** page for that space.

Note:

- Spaces created in Meeting Management will not be visible in web app.
- Spaces created in web app will be in view only mode and cannot be edited or deleted in Meeting Management
- After a space is renamed, Meeting Management prevents the creation of a new space using the old name, even though the original space no longer uses the old name.

5.1.3 Editing spaces

Only those spaces created by the administrator or video operators using Meeting Management can be edited. Space name can be modified using the ✎ edit icon.

Video operators can edit the space created by them or those they are tagged with; however, administrators can edit spaces created by the video operators.

The following table explains all the access enabled for tagged and untagged video operators for the spaces created in Meeting Management:

Table 2: Access enabled for tagged and untagged video operators for the spaces created in Meeting Management

Users	Tagged spaces	Untagged spaces
Tagged video operator	Access to view, edit, delete	No access
Untagged video operator	No access	Access to view, edit, delete

To modify the join information used by the members to access the space:

1. Click edit icon to launch **Edit access role** pop-up window.
2. Make necessary changes to **Passcode**, **Visibility** and **Video address**.

   Note:
   - The new passcode entered should be an integer value and must contain a minimum length as defined in the dial-in security profile in space templates.
   - In case the entered video address is already available in Meeting Server, administrator will be prompted to enter a different video address.

3. Click the **Save** button.

5.1.4 Deleting spaces

Administrators can delete only the spaces created in Meeting Management. Video operators can delete only the spaces created by them or those they are tagged to in Meeting Management. Delete icon available against the space name can be used to delete space.

5.1.5 Join information

The **Join information** tab displays the meeting details: Visibility, Meeting ID, Passcode, and Video address. You can obtain join information as email template and share it with the participants by copying the join information using icon available against each role.

Note:
- The administrators can view, edit and delete the spaces created by the video operators.
- Meeting Management will display the join link only if the port is configured in the Meeting Server.

5.1.6 Edit access role

You can edit this information and set preferences for visibility of the space by selecting one the following options from the Visibility drop down:

- In public directory, visible to all space members and call participants
- All call participants and space members
- All space members
- Space owner only

5.2 Blast dial configuration

Blast dial can only be configured for clusters where Meeting Management is setup to manage meetings on that cluster.

- If the cluster is not managed by Meeting Management, you will see the following message:

  Blast dial cannot be configured on this space because this Meeting Management does not manage meetings on this cluster. To change this, visit Servers and edit this cluster.

  Go to **Server settings** and under **Edit Cluster**, check the **Use Meeting Management to manage meetings on this cluster** check box.

- If Blast dial monitoring is turned off, you will see the following message:

  Blast dial cannot be configured on this space because this Meeting Management has blast dial monitoring turned off. To change this, visit Settings > Blast dial monitoring.

  Go to Settings and under Blast dial monitoring, change the settings.

5.2.1 Configurations

You can set the following configurations in the landing page:

- **On / Off**: You can turn on or turn off the blast dial feature at the Blast dial configuration landing page. When you turn it On, the other configuration options appear.
- **Retries**: This setting allows you to configure retry attempts if the contact does not connect to the call the first time.
  - **Number of retries**: The maximum number of times the system will attempt to dial out a contact if they fail to connect to the call.
  - **Time after a failed retry**: The minimum amount of time the system waits before retrying to dial out a contact. The default is 180 seconds.
- **Automatic join for blast dial participants**: You can on or off the audio prompt both at the global level and at the participant level. If the audio prompt is disabled, the audio prompt **Press 1 to enter the meeting or * to hang up** will not be played and the participant need not press the DTMF digits and enter the meeting when they accept the call. Administrators can also disable the audio prompt for specific participants in the meeting using the 📣 icon available for each participant.

  Note: Enabling or disabling the audio prompt at global level overrides the setting at the participant level.

5.2.2 Adding dial-out contacts

There are two ways to add participants to the list of blast dial contacts. You can either manually add them one at a time using the **Add contact** button or you can use the CSV option to upload a CSV file containing details of the contacts, such as name and video address.

Add contact

To add a contact:

1. Click on **Add Contact**. The **Add dial-out contact** window opens.
2. Enter the name and address of the contact.
3. Enable or disable the audio prompt option using **Require prompt to connect participant.**
4. Click **Done**. The contact details get added to the list of contacts. You can edit or delete the contacts from the list using the associated buttons.

Upload CSV

To upload a CSV file:

1. Click on the **CSV** drop down to upload a .csv file containing name, address and audio prompt options of contacts.

   Tip: You can download a blank CSV template and use that file to add the contacts and corresponding audio prompt options.

2. Upload the CSV file using the **Upload CSV** option.

   Note: If you have already added contacts using either of the options, the added contacts will be overwritten and only the newly uploaded CSV contacts will be added.

3. When the file is uploaded, the **Download CSV** option is enabled. In the **CSV** drop down, you can select **Download CSV** to download the existing CSV, edit the content, and upload it again.

Note:
- If the CSV file contains invalid characters, is in the wrong file format, exceeds the maximum file size, or contains more than the allowed number of contacts, an error message with the suggested resolution is displayed. Follow the instructions in the message to correct the errors and upload the file.
- The audio prompt value provided in the .csv file is case sensitive and will be disabled by default if an invalid value is entered or left blank.

6 Users - Add users or edit user settings

6.1 About users

Meeting Management supports locally managed users as well as user authentication via LDAP. You can choose to have only local users, only LDAP users, or both.

- **Local users** are added and managed locally on the Meeting Management **Users** page. These users are authenticated directly by Meeting Management.

  One local administrator user is generated during installation, and you can add more users after you have signed in for the first time. Local users are useful for setup and test, and for making LDAP changes without getting locked out of Meeting Management.

- **LDAP users** are added via mappings to existing groups on your LDAP server. Meeting Management uses your LDAP server to authenticate these users by checking their group membership when they sign in.

  Authentication via LDAP is recommended for general use and administration.

We recommend that you maintain at least one local administrator user account. This ensures continued access to Meeting Management in the event of LDAP issues. For general production use, we recommend that users are authenticated via LDAP. If authentication issues occur, LDAP users can reset their passwords on the LDAP server and then log in to Meeting Management again. Local users can reset their credentials with the assistance of other administrators. If the local administrator encounters authentication issues and they are the only administrator account available, the password cannot be recovered. In such cases, the local administrator user must re-install Meeting Management after removing all the existing data.

Note: The LDAP attribute name is case sensitive.

Users can have two 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. Administrators can tag video operators to specific spaces, giving them access to the meetings associated with those spaces only.
- **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. Video operators will have permission to perform the tasks related to meetings held in the space as assigned by the administrator.

For local users, the role is assigned to their user profile.

For LDAP users, the role is assigned to the LDAP group they belong to. If one user is in several groups with different roles, then this user will be assigned the administrator role.

6.2 Edit LDAP server details

LDAP server details are entered during the installation process. For details, see the *Installation and Configuration Guide*.

If you need to edit the details for your LDAP server or to replace the certificate, we recommend that you sign in as a local administrator user. This is to make sure that you can still sign in if there should be any issues with the details.

To edit LDAP server details:

1. Sign as a local administrator.
2. Make any relevant changes.

   See the installation guide for requirements and detailed instructions.
3. Scroll down to the **Authorization** section and enter the password for your LDAP bind user.
4. **Save** the changes and **Restart** Meeting Management.

Note: You can restart now or wait until you have completed the configuration.

6.3 Assigning spaces to video operators

Meeting Management administrators can tag video operators to specific spaces, giving them access to the meetings associated with those spaces only. Administrators can now limit video operators' access to all spaces and meetings by adding tag(s) while creating or modifying video operators. This allows them to manage and monitor the meetings more effectively.

Meeting Management administrators can view all the meetings and spaces (with or without tags) using the **Meetings** or **Spaces** tab respectively. Tags can be added only to video operators.

Tags can be created by administrators in Meeting Server only, using the coSpace API. Refer to Meeting Server API Guide for more details. Space tags can be added to both new and existing video operators.

In this feature:

- A video operator can be given access to multiple spaces and meetings by assigning multiple tags. A video operator can be assigned a maximum of 10 tags.
- Tags added or modified to a space/video operator during a session, will reflect only after the video operator signs in for the next session.
- Video operators have permission to perform the tasks in meetings held in the space as assigned by the administrator.
- The usernames for administrator and video operator must be unique.

- It is recommended to use different usernames for both Local and LDAP user group to avoid the tags from being assigned incorrectly.
- On removing/disconnecting any LDAP user group from Meeting Management and then adding it back, Meeting Management continues to retain the tags assigned by the administrator to that LDAP user group.

6.4 Add LDAP groups

LDAP user groups are configured on your LDAP server and mapped to Meeting Management, so Meeting Management can use the LDAP server to authenticate user by checking their group membership when they sign in.

See more about users and LDAP user groups in the Before you start article.

6.4.1 Add LDAP user groups

To add a user group:

1. On the **Users** page, go to the **LDAP user groups** tab.
2. Click **Add LDAP group**.
3. Enter **LDAP path**.
4. Click **Check** to see if the group is found.
5. If the group is found, click **View users** to check if you see the usernames you expected to see in this group.
6. Select a role for the group.
7. Click **View User Profile** button available in **Actions** against the selected user to launch **User Profile** pop-up window.
8. Assign tags (optional) in **Add tags** field. A maximum of 10 tags can be added.

   This enables administrators to assign tags to video operators, giving them access to only those meetings they are tagged to.
9. Click **Next**.
10. Optional: **Copy link** so you can send it to your users.

    The link you see here is your CDR receiver address. If your team has chosen to provide a different address to users for accessing the browser interface, then give them that address instead.
11. Click **Done**.

12. Restart Meeting Management

Note: You can restart now or wait until you have completed the configuration.

6.5 Set up security policies for local users

You can set up security policies for local users on the **Users** page, **Local configuration** tab.

You can set up the following policies:

- **Enforce password policy** to require a minimum password length

  This is disabled until you select it. The default minimum length is 8 characters

- **Use a passphrase generator** to enable a built-in passphrase generator

  The built-in passphrase generator combines words from a dictionary to suggest new passwords. The default number of words in a passphrase is 5, and you can choose any number between 1 and 8.

  If you want to use the built-in passphrase generator, you need to provide a dictionary.

  Dictionary requirements:

  - *The dictionary must be a text file with one word in each line.*
  - *Characters must be UTF-8 encoded.*
  - *The file must not contain any null characters .*
  - *Maximum file size is 10 MB.*

- **Enforce password reuse policy** to restrict password reuse

  This is disabled until you select it. The input fields are blank until you enter a value.

Note: Changes to the security policies only take effect after you **restart** Meeting Management.

Note: Note that **Enforce password policy** and **Enforce password reuse policy** are applied only when users change their own password.

Note: If the passphrase generator is enabled, Meeting Management will suggest passphrases for all users.

- **Use a passphrase verifier** to check the quality of user password against a dictionary containing commonly used words, repetitive or sequential characters.

  The list will also include context specific words, such as service name, username, product name, and derivatives.If the user chosen password matches one from the list, the passphrase verifier rejects the password and notifies the user to choose a different value.

  Dictionary requirements:

  - *The dictionary must be a text file with one word in each line.*
  - *Characters must be UTF-8 encoded.*
  - *The file must not contain any null characters .*
  - *Maximum file size is 10 MB.*

  To enable passphrase verifier:

  1. Scroll down to **Use passphrase verifier** and check the checkbox.
  2. Click **Upload dictionary** button and select a text file (.txt) containing a list of passphrases that do not meet the security requirements.
  3. To remove existing dictionary file, click **remove**.

Note:
• Meeting Management does not provide a default dictionary. The administrators must define the dictionary and upload it.
• If a dictionary is present when backing up Meeting Management, it will be included in the backup file. When the backup file is restored, the dictionary will also be restored.

- **Enforce password complexity** to check the strength of the password. You may set the level of complexity required in passwords when users create them.

  *While adding or editing a local user, if the password set by the user in **Add Local User** pop-up window does not meet the complexity criteria configured by the administrator, Meeting Management notifies the user to include the necessary character(s) to meet the password strength.This is disabled until you select it.*

  *While setting up security policies for users, select any or all of the following options in **Enforce password complexity**:*

  - Contain upper-case letters (A-Z)
  - Contain lower-case letters (a-z)
  - Contain at least one number (0-9)
  - Contain at least one special character (!$%^&*()_+|~-={}[]:";'<>?,/)

  To enable password complexity:

  1. Scroll down to **Enforce password complexity** and enable the **Enforce password complexity** checkbox.
  2. Select the checkbox options that are necessary in the user's password.
  3. Click **Save**.

- **Enforce password expiration** to configure the duration (in days) a password can be used. When the password expires, Meeting Management notifies the user to create a new password when the user logs-in after the current password is expired.

  *When there are 7 days or fewer left until password expiry, a warning message will be displayed in the **Notifications**, notifying the local user of the upcoming password change that is required. However, if the password is expiring within 24 hours or less, an error message will be displayed, requiring the password to be updated immediately. In case password expiry period is configured as 7 days or less, then only error messages will be displayed, and the warning message feature will be disabled.*

  If the password is not changed even after receiving the notification, Meeting Management notifies the user to create a new password when the user logs-in after the current password is expired.

  This is disabled until you select it. The input fields will have 30 days as default value.

  To enable password expiration:

  1. Scroll down to **Enforce password expiration** and enable the **Enforce password expiration** check-box.
  2. Enter the number of days in the **Maximum age of password (in days)** field.
  3. Click **Save**.
  4. Restart Meeting Management

  Note: When password expiration is enabled for the first time, all local users passwords will be expired and the users will have to change the password.

- **Enforce change password for first log-in** to ensure secure access by prompting users to change their password on their first log-in.

  *When a user logs in for the first time or an administrator resets their password, Meeting Management prompts the user to set a new password, with a message **Please set your own password now.**. The user has to provide new password twice to confirm that the intended password is correctly configured.*

6.6 Add local users

You can add, remove, or edit local user accounts on the **Users** page, **Local** tab.

See more about users in the Before you start article.

To add a local user:

1. On the **Users** page, go to the **Local** tab.
2. Click **Add local user**.

3. Enter a username.

   Note: The username cannot be changed later, so check carefully before you save the details.

4. Optional: Enter first and last name.
5. Assign a role.
6. Create a new password.
7. Confirm password and click **Add**.
8. In **Add tags** field, enter the tags. A maximum of 10 tags can be added.

   This enables administrators to assign tags to video operators, giving them access to only those meetings they are tagged to.

To delete a local user:

1. On the **Users** page, go to the **Local** tab.
2. Find the user you want to delete, and click  in the **Actions** column.

Note: You can never delete the administrator account you are currently signed in with.

If you only have one local administrator user account and you want to delete it, then sign in as an LDAP administrator to delete the local account.

To edit a local user:

1. On the **Users** page, go to the **Local** tab.
2. Find the user you want to edit, and click the **User profile** button  in the **Actions** column.
3. Make the necessary changes.
4. Click **Done**.

In case of authentication issues, local users can reset their credentials with the assistance of other administrators.

To unlock a user:

1. On the **Users** page, go to the **Local** tab.
2. Find the user you want to unlock and click the **Unlock** button in the **Actions** column.
3. Make the necessary changes in the password.
4. Click **Done**.

7 Servers - add or edit Servers

On the **Servers** page you can view and edit all your connected Meeting Server Call Bridges and Edge Nodes. You can also add new Call Bridges.

Once the deployment of a server is successful, you can view all the successfully configured servers in **Configured Servers** tab. The servers with failed or pending deployment status will be displayed in **Partial Configured Servers** tab.

You can edit or remove details for a cluster, such as whether you want to disable meeting management. For each cluster, you can set up provisioning of users and create space templates, you can associate the cluster with TMS to see upcoming meetings in Meeting Management. If you or another user has already used Meeting Management to set up provisioning, but did not commit the changes, you will see a notification banner for the cluster with a link that sends you to the **Provisioning** page, Review and commit tab for the cluster.

Your Meeting Management connects to Meeting Servers via the Call Bridge API. If you did not set up an API user account on each Call Bridge for your Meeting Management, please do that before you continue. For instructions, see "Accessing the API" in *Cisco Meeting Server API Reference guide*. You can find it on the Programming Guides page on cisco.com.

Also, if your CDR receiver address is not set correctly your Meeting Management cannot receive all the relevant information about active meetings, which you need if you enable the meeting management functionality.

To add a Call Bridge or Edge Node:

1. On the **Servers** page, click **Add Server**.
2. Choose one of the following:
    a. Add Configured Server:
    b. Configure New Server:
3. Click **Ok**.

7.1 Add Configured Server

You can add a Call Bridge Server that is already configured for managing licensing and other services or add an existing Meeting Server Edge Node.

If you chose **Add Server** and add an existing Meeting Server Call Bridge or Edge Node Server, follow the steps in this section. Enter the information for Cisco Meeting Server connection settings:

1. In the **Server address** field, enter the IP address or FQDN (fully qualified domain name) for your Call Bridge or Edge Node Server.

   This is the same as your Web Admin Interface address.

   Note: If you type in IPv6 addresses, use square brackets.

2. In the **Port** field, enter the port number for your Call Bridge or Edge Node Server.

   Note: If you leave this field empty, Meeting Management will use port 443.

3. Enter the MMP administrator **Username** and **Password** to add the Call Bridge or Edge Node Server.

   Note: For security and auditing reasons, we strongly recommend that you use a dedicated administrator account for Meeting Management.

4. Enter a **Display name**.

   You can choose any display name you want. Keep in mind that it must make sense to other administrators and to video operators.

5. Optional: check **Use a trusted certificate chain to verify** if you want to use certificates.

6. Optional: check **Certificates against certificate revocation lists (CRLs)** if you chose to use certificates, and you want Meeting Management to reject the connection if a certificate has been revoked.

   Meeting Management will block the connection if a certificate in the chain has been revoked, or if there is a CRL it cannot access.

   We recommend that you enable this when possible.

   Note: Only certificates with HTTP Certificate Distribution points (CDPs) are supported. If you are using CRL checks, and a certificate has no CDP, or if the CDP is not reachable via HTTP, then the connection is rejected.

   Also, Meeting Management must be set up so it can connect to external address via HTTP.

7. Optional: If you have chosen to use certificate security, then **Upload certificate**.

   Certificate requirements:

   - *The certificate chain should include the certificate of the CA that signed the Web Admin Interface's certificate, plus any certificates higher in the certificate chain, up to and including the root CA certificate.*
   - *The server address you entered for your Call Bridge or Edge Node must be included in the Web Admin Interface certificate.*

   Note: If the SAN (Subject Alternative Name) field is used, Meeting Management does not look at the Common Name, so make sure that the server address is added to the SAN field.

8. Optional: If you want to use Meeting Management only for licensing and provisioning, then uncheck the **Use Meeting Management to manage meetings on this cluster** check box.

9. Note: You can change this later by editing cluster settings, see Disable meeting management for a cluster.

10. Note: There is no information on the Meetings page to let video operators know that meeting management had been disabled for one or more clusters.

11. Click **Add**.
12. Optional: **Edit cluster** to give it a display name that makes sense to you as well as all other users.

If the Call Bridge or Edge Node you added is part of a cluster, the other Call Bridges or Edge Nodes in the cluster are auto-discovered and displayed below so you can easily add them.

To add auto-discovered Call Bridges and Edge Nodes:

1. Click **Show**.
2. In the **Actions** column, click ＋.
3. Enter details for the Call Bridge or Edge Node and upload certificate if relevant.
4. Continue until you have added all Call Bridges or Edge Nodes in the cluster.

To edit a Call Bridge or Edge Node:

1. Scroll down to the Call Bridge or Edge Node you want to edit and click or click anywhere in the row.
2. Edit any other details.

3. To reset the password, click the **Reset password** button to launch the **Reset Password** pop-up window. The following fields are displayed:
    a. **Username** – Displays the MMP administrator Username.
    b. **Current password** – Enter the password that is currently configured. This field will not be displayed if the **CMS password** reset option in the **Advance security** tab is checked.
    c. **New password** – Enter the new password for the Meeting Server. Meeting Management validates the new password against the criteria defined in the Meeting Server and displays error messages in case of invalid entries.
    d. **Confirm new password** – Re-enter the new password.
4. Click **Done**

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

To disable or enable the Meeting Management functionality for an existing cluster:

1. Click **Edit cluster**
2. Check or uncheck the **Use Meeting Management to manage meetings on this cluster** check box
3. Click **Done**.

7.2 Configure New Server

If you chose **Add Server** and select **Configure and add a new Meeting Server (Call Bridge)**, Installation Assistant opens on the Meeting Management console.

7.2.1 Staging

To configure a new Meeting Server, ensure that these factors are addressed:

- the Meeting Server is empty
- configure the Meeting Server DNS entries

New Meeting Server Instances

The Meeting Server must have its Virtual Machine deployed and running, an admin account enabled, and it's IPV4 'a' interface configured. No other configuration should be performed. The Installation Guide for Cisco Meeting Server 1000 and Virtualized Deploymentsdescribes how to deploy a Meeting Server instance or configure a Cisco Meeting Server 1000 appliance. The chapter, **Setting up Network Interface for IPv4** in the guide describes configuring the server. DO NOT go beyond the step for configuring the 'a' interface.

Existing Meeting Server Instances

If a Meeting Server instance has been previously configured or has been used with the Installation Assistant tool but not completed its configuration successfully, it must be reset and set to the same configuration state as a new server before it can be used with the Installation Assistant. You cannot use Installation Assistant on top of a prior configuration. To reset the server:

1. Log into the MMP interface of Meeting Server with an administrator account and issue the command **factory_reset full** and confirm when prompted. The server will reset itself to default configuration and reboot.
2. Log into the MMP interface of the Meeting Server and login with username **admin** password **admin**.
3. Set a new admin password when prompted.
4. Configure the ipv4 settings for the 'a' interface. See the 'Installation Guide for Cisco Meeting Server 1000 and Virtualized Deployments.'

Note: When following the configuration steps in the above guide, DO NOT go beyond configuring the 'a' interface.

7.2.2 Adding a new Meeting Server

To complete server configuration tasks you will also need:

- Addresses for your network's DNS and NTP servers
- The address of the SIP Proxy you will use with Meeting Server
- The SIP domain picked out that you will use with Meeting Server
- If configuring user imports, you will need the connection details to your network's LDAP directory including location, credentials, and LDAP user location details.
- If configuring the server with certificates (recommended) you should have a FQDN picked for the Meeting Server and defined in your DNS server records.
- If configuring the server with certificates (recommended) you will need to have your certificate request signed by your Certificate Authority of choice. The Installation Assistant can help generate the certificate request or you can use an existing certificate and key pair.

The major steps for configuring a new Meeting Server are as follows:

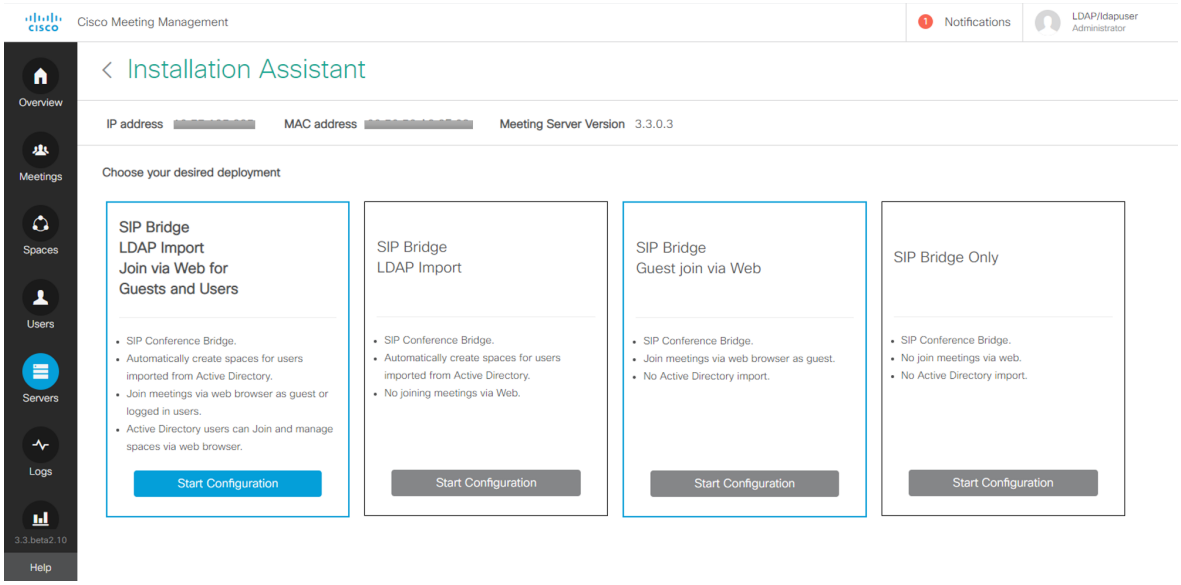
1. In the **Installation Assistant** page, enter **Server address** of the Meeting Server.
2. Enter the **Username** configured on the Meeting Server.

   Note: By default, '**admin**' is used as the username.

3. Enter the **Password** configured on the Meeting Server.
4. Click **Connect**.

   Note: The **Connect** button is enabled, only after the server address, username and password details are given.

5. Choose your desired deployment from the following options and then click **Start Configuration**. Based on your selection of deployment type, a wizard based interface is defined and displayed for configuring the server.
    a. **SIP Bridge LDAP Import Join via Web for Guests and Users**: The wizard navigates through all the steps of the configuration.
    b. **SIP Bridge LDAP Import**: The wizard navigates through all the steps of the configuration except Web Bridge.
    c. **SIP Bridge Guest join via Web**: The wizard navigates through all the steps of the configuration except Conferencing User.
    d. **SIP Bridge only**: The wizard navigates through all the steps of the configuration except Web Bridge and Conferencing User.



6. Navigate through the wizard by entering the required information as prompted. Once all fields are validated, the **Next** button is enabled.
7. The wizard navigates through all or some of the following pages depending on the deployment type selected:
    - Certificate
    - Network
    - Call Bridge
    - Web Bridge
    - Conferencing User
    - Security
    - Push Configuration

8. Review your settings and when ready, click '**Push Configuration**' to push the configuration to the Meeting Server.

   Note: If there is a problem pushing the configuration to the server, you can navigate to the **Logs** tab and download Meeting Management logs using **Download Log Bundle** to diagnose the issues.

8 Certificate

The Certificate panel allows you to select which method to specify the X.509 certificate necessary for Meeting Server, and provides a guided process to create new certificate requests for those looking to create new certificates. The Installation Assistant supports using both certificates signed by a Certificate Authority and the use of self-signed certificates. The certificates panel will automatically adapt the options shown based on your selection of using CA signed certificates or self-signed certificates.

Note: Self-signed certificates are not supported for all functionality, they are a security risk and are not recommended.

The recommended path is to use a X.509 certificate signed by a Certificate Authority trusted by your organization. The Certificate Authority can be an internal or public certificate authority. For more details on how Meeting Server uses certificates and their requirements, please refer to the Cisco Meeting Server, Certificate Guidelines Single Combined Server Deployments Guide.

8.1 CA Signed Certificate

When the CA Signed Certificate method is selected, there are two available paths:

- **New Certificate via CSR** – The Installation Assistant will guide you through creating a certificate signing request to supply to your Certificate Authority, and they in turn will supply you with a signed certificate.
- **Supply an existing certificate and key** – Upload an existing certificate and key pair you have prepared external to Installation Assistant.

8.1.1 New certificate via CSR

This option guides you through creating a new certificate by creating a Certificate Signing Request (CSR) to provide to your Certificate Authority.

Completing this process requires:

1. Providing details for the certificate in the Installation Assistant and downloading the resulting CSR file.
2. Supplying the CSR to your Certificate Authority and they will return a signed certificate. You will also need the chain of public certificates that represents the Certificate Authority, which they will provide.
3. The resulting files are then uploaded to the Installation Assistant which will handle configuring Meeting Server with the supplied files.

Note: You are free to close the Installation Assistant tool after downloading your CSR. Once you have obtained the signed certificate from the Certificate Authority, navigate to **Partial Configured Meeting Server** tab in **Servers** page in and click **Resume** to return to the **Certificate** panel to complete the certificate upload process (see step 4 below).

Steps for creating a new certificate request (CSR):

1. In the Certificate Panel, select **Certificate Type** as **CA Signed**.
2. In the **Certificate Upload Options**, select **New Certificate via CSR**.
3. Complete the fields with the details to use for your Meeting Server. The fields are described below. When complete, click the **Next** button to return to the certificate panel. The **Next** button is only enabled after you have entered all the required details.

   Note: If there is an existing generated certificate, and you click **Regenerate CSR** then the existing file will be over written with the new details, as Installation Assistant does not allow multiple CSR files to be generated.

   Table 3: Fields required for a Certificate Signing Request

Field Name	Description	Values
FQDN for Meeting Server	It is the CN value for your certificate and must be defined in the DNS server.	Enter the FQDN of the server.
SIP domain for Meeting Server	It is recommended to use a sub-domain.	Enter the SIP domain of the server to align with the routing rules.

4. The completed CSR will be shown in the Certificate Panel. Click **Download CSR** to save the resulting CSR to a file on your local drive.
5. Give the CSR to your Certificate Authority to be signed. They will return a signed certificate file. You will also need the certificate chain bundle for that Certificate Authority.
6. Once you have your signed certificate and certificate chain files, return to the Certificate Panel if necessary and select **Upload Files** to upload the Certificate/ Bundle. Two fields are shown to specify the certificate and CA certificate chain. Use the **Select File** link to locate the specific file on your local computer. The certificate files must have one of the following extensions (CER,CRT,PEM,DER) and must be encoded as PEM or DER.
7. Once both files are specified, click **Next** button and the files will be sent to the Installation Assistant and validated.
8. If successful, the Certificate panel will be marked as complete in the wizard and you will be navigated to the Network panel.

Error Scenarios

An error message is displayed and the **Next** button is disabled in case of the following scenarios:

- If the upload fails due to server/ technical issue.
  Solution: You must re-upload the certificate files.
- If the given certificate is incorrect.
  Solution: You have to select and upload the correct certificate and CA certificate chain.
- If the certificate fails to upload.
  Solution: Re-upload the certificate with the correct FQDN/SIP domain or correct key usage.
- If the certificate chain fails to upload.
  Solution: Re-upload the certificate chain with the correct FQDN/SIP domain or correct key usage.

8.1.2 Use Existing Certificate and Key

Installation Assistant provides you with an option to utilize an existing private key and signed certificate for the Meeting Server, rather than generate a CSR via the tool. This is done by using the option **Supply an existing certificate and key**.

You are required to provide the certificate, private key, and CA certificate chain. The certificate files must have one of the following extensions (CER,CRT,PEM,DER) and must be encoded as PEM or DER.

Steps for using an existing certificate:

1. In the Certificate Panel, select **Certificate Type** as **CA Signed**.
2. In the **Certificate Upload Options**, select **Supply an existing certificate and key**
3. Five fields are shown for specifying the **FQDN for Meeting Server**, **SIP domain for Meeting Server**, **Private key**, **CA certificate chain**, and **Certificate**. Use the **Select File** link to locate the specific file on your local computer. The certificate files must have one of the following extensions (CER,CRT,PEM,DER) and must be encoded as PEM or DER.
4. Once all five files are specified, the **Next** button is enabled. Click **Next** and the files will be sent to the Installation Assistant and validated.

If successful, the Certificate panel will be marked as complete in the wizard and you will be navigated to the Network panel.

Error Scenarios

An error message is displayed and the **Next** button is disabled in case of the following scenarios:

- If the upload fails due to server/ technical issue
  Solution: You must re-upload the certificate files.

- If the given certificate is incorrect, the **Upload** button is disabled.
  Solution: You have to select and upload the correct certificate and CA certificate chain.
- If the provided FQDN is incorrect.
  Solution: You must enter a valid FQDN.
- If the provided SIP domain is incorrect.
  Solution: You must enter a valid SIP domain.

8.2 Self Signed Certificate

Self signed certificates are certificates that are signed by the local entity. There is no governing authority validating the certificate. Self-signed certificates are valid, but not recommended due to lack of security. For more information on how Meeting Server uses certificates and their requirements, please refer to the Cisco Meeting Server Certificate Guidelines.

Note: Self signed certificate details are not stored by the tool, hence it is recommended that you complete the configuration in one go.

Note: If you are using self-signed certificates to configure the Meeting Server, ensure that the Meeting Server time is the current time. If the Meeting Server time is not in sync with the actual time, then an error is displayed. You must set the time correctly by using the date MMP command. The default system time is in UTC.

Steps for using a self-signed certificate:

1. In the Certificate panel, select **Self signed**.
2. Enter the **FQDN for Meeting Server**.
3. Enter the **SIP domain for Meeting Server** to align with the routing rules.
4. The **Next** button is only enabled after you have entered all the required details. Click **Next** and the files will be sent to the Installation Assistant and validated.
5. If successful, the Certificate panel will be marked as complete in the wizard and you will be navigated to the Network panel.

Error Scenarios

An error message is displayed and the **Next** button is disabled in case of the following scenarios:

- If the provided FQDN is incorrect.
  Solution: You must enter a valid FQDN.
- If the provided SIP domain is incorrect.
  Solution: You must enter a valid SIP domain.

9 Network

The Network panel allows you to configure the core network settings for the server.

Note: You may need to contact your network administrator for guidance on these settings.

1. Configure the following:

Table 4: Description of the fields to be filled ffor configuring network settings

Fieldname	Description	Action
NTP Server	You need to configure at least one NTP server by giving either FQDN or IP address. Note: You can configure up to 5 NTP servers.	Click '**Add server**'. The address of your NTP server is added to Cisco Meeting Server
Time zone	Local time zone of your server	Select your preferred timezone.
DNS server	You need to configure at least one DNS server by giving the IP address. Note: You can configure up to 5 DNS servers.	Enter the IP address of the server and click '**Add server**'. The address of your DNS server is added to Cisco Meeting Server
Webadmin port	Configure the TCP port number that the Meeting Server Web Admin Interface listens on. If you are using a deployment that includes Web bridge then you are not allowed to use port 443.	Enter the port number.

Ensure that all the details are entered and the configuration of the Network panel is successfully completed. The **Next** button is enabled and the network settings are saved, click on it and you are navigated to next panel based on your chosen deployment.

9.1 Deleting a DNS or NTP server

1. Click to delete the DNS/ NTP server.

Error Scenarios

An error message is displayed and the **Next** button is disabled in case of the following scenarios:

- If an already entered NTP server address is provided.
  Solution: You must provide a valid IP address/ FQDN.
- If an incorrect DNS server address is provided.
  Solution: You must provide a valid IP address.
- If an incorrect port number is provided.
  Solution: You must enter a valid port number.
- If an already entered NTP server address is provided.
  Solution: You must provide a different IP address/ FQDN.
- If an already entered DNS server address is provided.
  Solution: You must provide a different IP address.

10 Call Bridge

The Call Bridge panel allows you to configure the settings for the Call Bridge service.

1. Enter the following details:

Table 5: Description of the fields to be filled for setting Call Bridgeservice

Field Name	Action
SIP Proxy	Enter the FQDN or IP address of the SIP Proxy that will receive outbound calls from the Meeting Server.
Encryption	Select the encryption mode (TLS) for the connection.
Media encryption for SIP calls	Select the required option from the drop-down list.
ActiveControl	Enable ActiveControl permissions for all the participants. When this option is enabled, it creates a **callLegProfile** and **systemProfile** to enable ActiveControls for participants by default. Note: these settings are not enabled by default in the Meeting Server.

2. When the correct details are provided, the configuration of the Call Bridge panel is successfully completed.

Note: Ensure that all the details are entered to save your settings successfully.

3. The **Next** button is enabled and by clicking on it , you are navigated to the next panel, based on your chosen deployment.

Error Scenario

An error message is displayed and the **Next** button is disabled in case of the following scenario:

- If the entered SIP Proxy detail is incorrect.
  Solution: You must provide a valid IP address/ FQDN.

11 Web Bridge

The Web Bridge panel allows you to configure the Cisco Meeting Server Web App by opening the port that allows the Call Bridge to connect to the Web Bridge.

1. Enter the **Call Bridge to Web Bridge (c2w) listening port**. By default, the port number is 9999.
2. When the correct details are provided, the configuration of the Web Bridge panel is successfully completed.
3. The **Next** button is enabled and by clicking on it , you are navigated to the next panel based on your chosen deployment.

Error Scenario

An error message is displayed and the **Next** button is disabled in case of the following scenario:

- If the entered Call Bridge to Web Bridge (c2w) port detail is incorrect.
  Solution: You must provide a valid port number.

Note: It should not be 443 or the webadmin port.

12 Conferencing User

The Conferencing user panel allows you to import LDAP users to log into the Cisco Meeting Web App.

Creating user accounts requires:

- Defining the connection properties to connect to your Active Directory server. By default, LDAPS option is selected.
- Defining the search filter and field mapping values with which users are created on a Meeting Server. Installation Assistant has default values that works for most environments, but you have the option to override those defaults if necessary.

If you wish to create user accounts:

1. Fill in the **LDAP Connection Settings** fields with the values for connecting to your Active Directory controller. A **Next** button will be displayed once all required fields are completed.

   Details on each setting are provided in the following table:

Table 6: Configuring the LDAP connection

Field Name	Description	Inputs
Server address	The network address of the LDAP server to connect to.	The FQDN or IP Address of your LDAP server
Port	The TCP port on the LDAP server to connect to.	A valid port number. The default value is 636 for LDAPS and 389 for LDAP.
Username	The username of the user that will connect to the LDAP server. This user only needs read rights to the directory.	The LDAP Distinguished Name (DN) or UPN of the user to authenticate with. This field cannot be left blank
Password	The password of the user specified.	Password of the user. This field cannot be left blank.
Search base	The location in the LDAP directory from where import search queries will start from. For assistance with this value, contact your Domain Administrator.	The LDAP Distinguished Name (DN) of the directory location where searches should start. This field cannot be left blank
Assign PMP licenses to users	If enabled, imported users will be marked to be entitled to a PMP+ license. Do not enable if you have not purchased PMP+ licenses for all users being imported.	Enable to tag each imported user as having a PMP+ entitlement.
Override default user filter and field mapping details	Installation Assistant uses a default LDAP Search Filter and user field mappings that should work for most environments. This option when enabled, offers you the ability to view and customize these settings to fit your environment.	Enable to view or customize the LDAP search filter, and or LDAP user field mappings.

2. Click **Check LDAP Connection** button to make sure LDAP connectivity is available.

   Note: On clicking **Check LDAP Connection** button if the connection check fails, an error message is displayed: **LDAP Connection Failed**.

3. Once LDAP connectivity is established successfully, the **Next** button is enabled. Click **Next**

Note: Ensure that all the details are entered to save your settings successfully. If you are modifying the default values, ensure to use valid LDAP expressions used for the mapping.

Error Scenarios

- If on clicking **Check LDAP Connection** button, connection check fails
  Solution: You must provide valid LDAP connection details.

12.1 Customizing the LDAP Search and user mappings

Installation Assistant uses a default LDAP Search Filter and user field mappings that should work for most environments. The default, filters on users that have an email address defined, a username, and will set their Meeting Server username to their meeting address.

Enabling the override option will display the individual configuration fields used for import and show the settings Installation Assistant is using by default. When **Override default user filter and field mapping details** is enabled, users have the ability to customize these values to fit their environment.

The user mapping expressions define how to set the properties of a user when importing them into Meeting Server. The expressions use variables along with static text so that a user's properties in LDAP can be used when creating the user in Meeting Server. The use of LDAP properties is critical to ensure properties that are required to be unique per user (such as username or URI) are not duplicated. LDAP properties are referenced by their property name enclosed with the $ symbol. Example: The LDAP property 'mail' is referenced by $mail$ in the field mapping expressions.

Table 7: LDAP Import settings

Field Name	Description	Inputs
LDAP search filter	Defines the criteria of which LDAP users will be matched to be imported.	LDAP search string. Must use LDAP search syntax
Display name	The name shown for the user in directories and searches.	Mapping expression. Example: cn
User name	The username that the user will use to log into Cisco Meeting Web App. The resulting value must be unique across all users and spaces.	Mapping expression. Example: `$sAMAccountName$@company.com` This field cannot be blank and the result must be unique for each imported user

Field Name	Description	Inputs
Space name	Label given to space automatically created for user. Leave blank if not creating spaces for imported users.	Mapping expression. Example: **`$cn$ Meeting space`**
Space URI	Left hand portion of URI for the space automatically created for the user. Result must be unique per user and not conflict with usernames or other spaces. Leave blank if not creating spaces for imported users..	Mapping expression. Example: **`$cn$.space`**
Space secondary URI	Left hand portion of a second URI for the space automatically created for the user. Result must be unique per user and not conflict with usernames or other spaces. Optional field. Leave blank if not creating spaces for imported users.	Mapping expression. Example: **`$cn$.room`**
Space call ID	Sets the call ID for the space automatically created for the user. Result must be unique across all spaces. Optional field, Cisco Meeting Server will assign IDs automatically if left blank. Leave blank if not creating spaces for imported users.	Mapping expression.
Authentication ID mapping	Mapping property assigned to the imported user. Used in smartcard login scenarios. Leave blank unless specifically deploying certificate based logins.	Mapping expression. Example: **`$userPrincipalName$`**

The **Next** button is enabled. Click **Next** and the login credential is created, saved and you are navigated to next panel based on your chosen deployment.

Note: Ensure that all the details are entered to save your settings successfully.

Error Scenarios:

An error message is displayed and the **Next** button is disabled in case of the following scenarios:

- If the entered server address detail is incorrect.
  Solution: You must provide a valid IP address/ FQDN.

- If the entered port number is incorrect.
  Solution: You must provide correct and only numeric values.

13 Security

The Security panel allows you to create another user in the Meeting Server, if you lose access to your default administrator account.

1. Select **Create backup user account** to create a recovery account.
2. Provide the **New username**, **Password** and **Confirm Password**.

   Note: The **Password** must not be blank and **Username** should not be admin.

3. The **Next** button is enabled. Click **Next** and the login credential is created, saved and you are navigated to next panel based on your chosen deployment.

Error Scenarios:

An error message is displayed and the **Next** button is disabled in case of the following scenarios:

- If the entered username is incorrect.
  Solution: You must provide a valid username.
  Note: Enter an alphanumeric value other than 'admin'.

- If the entered password and confirmation passwords do not match.
  Solution: Re-enter the same passwords in both the fields.
  Note: You must provide only alphanumeric values.

14 Push Configuration

The Push Configuration panel allows you to review all the details of the respective panels that you have provided on Installation Assistant.

1. Click **Next** button to push the provided configuration details to the Meeting Server to complete the configuration process.
2. Once the configuration is pushed successfully to Meeting Server, the Installation Assistant displays the summary details. The added Meeting Server will be listed in **Configured Server** tab. You can edit or delete the added Meeting Servers by clicking the respective icons.

   Note: The added Meeting Server will be in expired license state. Ensure to add the Meeting Server to Meeting Management server.

3. To manage the meetings using the newly created Meeting Server cluster, you need to check **Use Meeting Management to manage meetings on this cluster** checkbox.
4. Enter **Display name**.
5. The **Exit** button is enabled. Click **Exit** to navigate to **Servers** page.
6. If the configuration was unsuccessful or incomplete, following are the possible next steps:
   a. Logs: You can navigate to **Logs** tab and use **Download log bundle** button to download Meeting Management logs, which will also include the Installation Assistant logs.
   b. Reset: You can use this link to remove the Meeting Server configuration pushed by the Installation Assistant.
   c. Resume: You can resume configuring a Meeting Server from **Partial Configured Server** tab.

The failed configurations are listed in the **Partial Configured Server** tab once you exit Installation Assistant.

14.1 SSH capability

SSH capability is required to perform tasks on the Edge Nodes added on Meeting Management. Administrators can connect to the SSH terminal and run MMP commands for the selected Meeting Server or Edge Nodes using the **SSH terminal** tab. You can select a Call Bridge or an Edge Node and connect to the SSH terminal by providing the MMP administrator credentials. Once connected you can run MMP commands on the selected server.

15 Disable meeting management for a cluster

If you only want to use Meeting Management for licensing and provisioning, then you can disable meeting management for individual clusters. This can be useful if you want to free up CDR capacity for other tools, if a cluster has tenants, or if a cluster hosts high volumes of meetings. See Meeting Management capacity in the *Installation and Configuration Guide*.

To disable meeting management for a cluster:

1. Go to the Servers page
2. Click Edit cluster
3. Uncheck the Use Meeting Management to manage meetings on this cluster check box.

   Meeting Management will no longer be a CDR receiver and events client on the Call Bridges in the cluster, and it will stop requesting information about meetings hosted on Call Bridges in the cluster.

   Note: For new clusters you can set this as part of adding the first Call Bridge in a cluster.

16 Provisioning

You can use Meeting Management to provision users and space templates on connected Meeting Servers.

You can access provisioning settings from the **Servers** page. For the cluster you want to set up provisioning for, you can click **Set up provisioning** to go to a page that lets you configure the provisioning settings.

16.1 What is a space?

A space is a virtual meeting room that participants can dial into to have audio or video meetings. All members of a space have access to the space and see it in their app, similar to a shared meeting room where all members have a key and can enter the room when they want. Others can be invited in for a meeting by the members of the space.

For more information about what spaces are and how the apps work, see the web app user guide and the visual "how to" guides. as well as the Important Information documents.

16.2 What is a space template?

A space template is a combination of pre-configured settings that can be used to create new spaces. The most basic settings are related to participants:

- What participant roles exist in the space, and which permissions each role has

  For instance, some participants can have a host or leader role and have full permissions to add or remove people, start recording, mute others, etc, while others have guest or staff roles with limited permissions. You can also have spaces with just one role where all members have the same permissions.

- Whether participant roles should be differentiated by their passcode, of if they should each have a unique URI and Meeting ID

There are also settings that are related to the behavior of meetings held in the space, such as the default layout, whether meetings are automatically recorded, whether there is a participant limit, etc.

16.3 Provisioning steps

Setting up provisioning consists of setting up LDAP filters, defining space templates and a few other settings, and committing the changes.

1. Before you start, get things ready.
2. Connect the cluster to LDAP servers.
3. Define which users to import.
4. Automatically create spaces.
5. Allow users to create spaces.
6. Review and commit your settings.
7. Start an LDAP sync to perform the provisioning.

16.4 Provisioning – Before you start

16.4.1 Supported LDAP implementations

The Meeting Server supports the following LDAP implementations:

- Microsoft Active Directory (AD)
- OpenLDAP
- Oracle Internet Directory (LDAP version 3)

For information about which versions have been tested with each version of the Meeting Server, see the Interoperability Database.

CAUTION: If you have set up LDAP via the Meeting ServerWeb Admin Interface then provisioning via Meeting Management will not work. Before you set up provisioning in Meeting Management, sign in to the Web Admin Interface, go to **Configuration**, **Active Directory** page, and empty all input fields, then click **Submit**. To avoid locking users out, do not synchronize before you have finished setting up provisioning on Meeting Management.

16.4.2 LDAP server details

For each LDAP server you want the Meeting Server cluster to connect to, you need the following:

- Protocol (LDAP/LDAPS)

  We recommend that you use LDAPS.

- LDAP server address
- LDAP server port number

  Defaults are 389 for LDAP, 636 for LDAPS. We recommend that you use LDAPS on port 636.

  If you want to use certificate verification: LDAP server certificate uploaded to the Meeting Serverand TLS certificate verification enabled.

- *We recommend that you use certificate verification. For information on how to do this, see the FAQ article How do I enable LDAP server certificate verification?.*
- Credentials for your LDAP bind user

  For security and auditing reasons, we recommend that you create a separate bind user account for Cisco Meeting Server.

16.4.3 User import details

For each group of users you want to import, you need:

- Base distinguished name (DN)
- LDAP search filter
- Sign-in user name mapping

  *This corresponds to what we call **Search attribute** when you connect an LDAP server to Meeting Management. It defines which LDAP attribute you want to use as the username that Meeting Server web appusers will use to sign in to the app. It must have a format similar to $sAMAccountName$@example.com, and the attribute must be one that is unique for each user.*

- Display name mapping

  This defines which LDAP attribute you want to be used as app users' display name. It must have a format similar to cn.

- Sufficient PMP Plus licenses

  The import settings for a group define whether the users in the group are assigned personal licenses. If you choose to assign the users personal licenses, then you need one PMP Plus for each user in the group.

  You do not need to install the licenses before you can provision users, but you need to install them before you start using the Meeting Server.

For more information about using LDAP with the Cisco Meeting Server, see the appropriate Meeting Server deployment guide. There is a section on LDAP configuration as well as an appendix with more information on LDAP field mappings.

16.5 Provisioning – LDAP servers

The first step of provisioning users and space templates is to connect the Meeting Server cluster to one or more LDAP servers that you want the Meeting Servers to import users from.

On the **Provisioning** page, **LDAP servers** tab, you can enter the details that the cluster will use to connect to the LDAP servers.

16.5.1 How to add an LDAP server

To connect the cluster to LDAP servers:

1. In Meeting Management, go to the **Servers** page and click **Set up provisioning**.
2. On the **LDAP servers** tab, click **Add LDAP server**.
3. Optional: Enter a server name that makes sense to you and other Meeting Management administrators.
4. Choose protocol.

   LDAP is for unencrypted TCP connections, LDAPS is for secure connections, optionally using the certificate trust store for authentication.
5. Enter server address and port number for the LDAP server.

   Default port numbers:

   - *LDAP: 389*
   - *LDAPS: 636*

   Note: You cannot upload a certificate via Meeting Management. To make an LDAPS connection fully secure, you must enable certificate verification on the Meeting Server and upload a certificate to its trust store. For instructions, see How do I enable LDAP server certificate verification?.

6. Enter **Bind DN** and **Password** for the LDAP server.

   These are credentials for the user account that will bind (authenticate) the Meeting Server cluster to your LDAP server.

7. Choose **Use LDAP paged results control** if you want the Meeting Server to receive search results in chunks, corresponding to pages in the LDAP library, rather than going through the whole database in one single operation.

   We recommend that you use paged results, unless you are using Oracle Internet Directory.

   Note: Paged results are not supported by Oracle Internet Directory.

Note: Your changes will not be applied before you have committed them. After you have committed the changes, template settings will take effect immediately. Changes to LDAP server details and any changes that affect users will take effect next time the Meeting Server is synchronized with the LDAP servers.

Note: All changes to provisioning settings that you have entered in Meeting Management will be lost if you restart Meeting Management before the changes have been committed.

16.6 Provisioning – Import users

As part of provisioning users and space templates on a Meeting Server cluster you must define which users to import from the LDAP servers that are connected to the cluster.

On the **Provisioning** page, **Import users** tab, you can add user imports, which are sets of LDAP filters and mappings that each define a subset of users to import from one of the connected LDAP servers.

16.6.1 How to add a user import

You can add as many user imports as you like. For each user import, you define subset of users to import from a specific LDAP server, you decide how their username and display names should be created, and you decide if you want to assign them a PMP Plus license.

We recommend that you make sure that the same users are included in only one user import. If PMP Plus licenses are assigned via one user import and not another, and a user matches the LDAP search filter for both user imports, then the user may or may not be assigned a PMP Plus license.

Note: If the same user is included in two different user imports, Meeting Management cannot control which user import the user will be associated with. This means that if a user is included in one user import that assigns PMP Plus licenses to users and is also included in a user import that does not assign any licenses, then you cannot control whether that user is assigned a license.

To define a subset of users to import:

1. Go to the **Servers** page and click **Set up provisioning**.
2. On the **Import users** tab, click **Add user import**.
3. Add a **Name** for the user import.

   We recommend that you choose a name that will make it easy for you and other administrators to distinguish this user import from others. If you leave the field blank, Meeting Management will create a name based on the settings you configure below.
4. From the drop-down, choose the LDAP server you want to set this user import filter for.
5. Enter **Base distinguished name**.

   The base distinguished name is the starting point for the directory search. The Meeting Server will search for LDAP groups in this node and all nodes below it in the LDAP tree.
6. Enter **LDAP search filter**.

   This filter defines the subset of users that you want to import.The syntax for the Filter field is described in rfc4515.

   Note: If you are using Active Directory, make sure that you enter a filter that only includes user objects.
7. Enter **Login user name mapping**.

   This defines which LDAP attribute you want to use as the username that Meeting Server web appusers will use to sign in to the app. It must have a format similar to $sAMAccountName$@example.com, and the attribute must be one that is unique for each user.

   Note: The LDAP attribute name is case sensitive.
8. Enter **Display name mapping**.

   This is the LDAP attribute that you want to use as participant name in meetings and on each web app user's own Home screen. It must have a format similar to cn.

   Note: The LDAP attribute name is case sensitive.

9. Check the **Assign Personal Multiparty Plus (PMP+) license to imported users** check box if you want to assign PMP Plus licenses to users who are imported based on these filter settings.

   If you prefer to use SMP Plus licenses, or if you want these users to only join meetings that have a different owner, then leave this check box unchecked.

Note: Your changes will not be applied before you have committed them. After you have committed the changes, template settings will take effect immediately. Changes to LDAP server details and any changes that affect users will take effect next time the Meeting Server is synchronized with the LDAP servers.

Note: All changes to provisioning settings that you have entered in Meeting Management will be lost if you restart Meeting Management before the changes have been committed.

16.7 Provisioning – Automatically create spaces

As a part of provisioning you can create spaces for users.

On the **Automatically create spaces** tab you can see all space templates that have been defined, and you can see which subsets of users will have spaces created with each template.

You can also create new space templates, and you can define which space templates to use to automatically create spaces. You can do this by setting up rules that map groups of users to space templates along with details of how space names and video addresses should be generated.

16.7.1 Add rules for automatically creating spaces

To define a rule:

1. Click **Add rule**.
2. Choose a user import from the **User import** drop-down.
3. Optional: Add a **Filter** to specify a smaller group of these users if you want to provision the same type of space to only some of them.

   You can leave the field blank if you want to provision the same type of space to all of the users in the chosen subset.

4. Define a **Space name mapping**.

   This defines a rule for how the space name will be generated. For instance, if you enter cn's space, and a user's Common Name is Sally Wood, then this user's space will be named Sally Wood's space.

   Note: The LDAP attribute name is case sensitive.

5. Define a **URI user part mapping**.

   This defines a rule for how the URIs for the space are defined. For instance, if you enter $sAMAccountName$, and a user's SAM account name is swood, and the domain for the user is example.com, then the URIs will be swood@example.com, swood.host@example.com, or similar, depending on how the unique URI generator for a role is defined.

   Note: The LDAP attribute used in the URI user part mapping must be unique for the user.

   Note: It is possible to use more than one LDAP attribute in the URI user part mapping. If you use more than one LDAP attribute, then make sure that at least one of them is unique for the user.

   Note: The Meeting Server will convert attribute values to lower case. No other characters are removed or modified (including spaces), so make sure that the URI user part mapping will result in a URI that can be used for all users.

6. Under **Choose a space template**, choose **Create new template** or choose an existing one.

   *If you chose an existing template, click **Done** and ignore the following steps.*

   *If you chose **Create new template**, click **Create space template** and continue to step 7.*

7. Define a **Template name**.

   Note: This name is also what users see in the Cisco Meeting Server web app. Make sure that you choose a name that would make sense to ordinary app users.

8. Write a space **Template description**.

   Note: This description is also seen in the web app, and they choose space templates based on this description. Make sure that you write a description that is easy for ordinary app users to understand.

9. Decide if different roles should be differentiated by their passcode, or if they should each have a unique URI and Meeting ID.
10. Click **Add role**
11. Enter a **Role name**.

    Note: Make sure that the name is descriptive so app users can guess from the name what this role is.

12. From the **Visibility** drop-down, choose the visibility scope for the template.
13. Enter a **Unique URI generator** to define a rule for how the Meeting Server should generate the URI that participants with this role should use to access the space.

    The URIs are created based on the URI user part mapping, the URI generator, and the domain. For example, if you entered $.host, and the URI user part mapping is $givenName$.space, then a space for someone named Sally created on the domain example.com will have the URI ***sally.space.host@example.com****.*

    Note: This field is disabled if you chose to use the same URI for all roles.

14. Define the minimum passcode length.

    If you ignore this setting, Meeting Management will choose to use the system default. If you do not want to require a passcode, then enter 0.

    Note: The system default is 0, unless your Meeting Server administrator has set a different default on system or tenant level.

    Note: If you have chosen to use the same URI and numeric ID for all roles, and there is more than one role, then you can only set one role to have no passcode. If you set more than one role to have no passcode, then the Meeting Server will ignore your setting for these and provide a 4 character passcode for them.

15. Click **Next**.
16. Check the **Make role and Activator** check box if you want participants with this role to be Activators.

    An Activator is a participant who can start a meeting. For information about scenarios where this is relevant, see "Use the meeting lobby and lock meetings" in the Cisco Meeting Management User Guide for Video Operators.

17. Define permissions for the role.

    *To use the system value for a setting, leave the **Override** check box unchecked.*

    *To define a new setting, check the **Override** check box and choose the value that you want from the following options:*

    Table 8: Options available while defining permissions for the role

Field name	Description
Maximum participants	Set a maximum number of active participants in the meeting.
Recording mode	Choose one of the following options: **Disable**: Recording is disabled **Manual**: Users can start and stop recordings **Automatic**: All meetings in the space are recorded
Locked by default	Set if all meetings in this space will start locked.
Passcode timeout (seconds)	Set the number of seconds the Meeting Server will wait for participants to enter a passcode when prompted before falling back to a role without passcode. To disable the timeout, enter a value of 0.
Video allowed	Set whether to allow participant video in meetings in this space. Sharing presentation video is always allowed, even for audio-only meetings.
Default video layout	Set the default video layout seen by participants in this meeting.
Behaviour when last activator leaves	The experience of remaining participants in the meeting when the last Activator leaves.
Allow change role	Participants with this permission can change role

18. Click **Next**.
19. Repeat steps 10-18 until you have added all the roles you want in this space template.
20. Use **Default for dial out** to select a default role for dial out participants during the meeting.
21. Click **Next**.
22. Define default settings for the space.

    *To use the system value for a setting, leave the **Override** check box unchecked.*

    *To define a new setting, check the **Override** check box and choose the value that you want.*

23. Click **Done**.

Note: Your changes will not be applied before you have committed them. After you have committed the changes, template settings will take effect immediately. Changes to LDAP server details and any changes that affect users will take effect next time the Meeting Server is synchronized with the LDAP servers.

Note: All changes to provisioning settings that you have entered in Meeting Management will be lost if you restart Meeting Management before the changes have been committed.

16.8 Provisioning – Allow users to create spaces

As part of provisioning you can decide which web app users will be allowed to create which types of spaces. This is done by assigning space templates to specific user imports, or to groups within a user import.

On the **Provisioning** page, **Allow users to create spaces** tab, you can create space templates and assign them to specific groups of web app users.

16.8.1 Limitations

- The user who creates a space is not assigned any of the roles that you define in Meeting Management. The space creator, who is also the space owner, will receive the default call leg profile for the space.
- The user who creates a space will be a member of the space.
- All members of a space will get the same call leg profile as the user who created it.
- When you make changes to a template, not all changes are applied to existing spaces.

  *New **Participant role settings** and **Space template settings** are applied to existing spaces. Other template changes, such as adding or removing roles, do not affect existing spaces.*

  If you want to make changes to existing spaces, you can do this manually via the API.

  Note: spaces that have been automatically created but have not yet been activated by the user do not count as existing spaces. An automatically created space will have the settings applied that are valid at the time the user activates it.

- The web app does not indicate to users if a template has been changed.

  We recommend that you update the name or the description when you make significant changes to templates that are already in use.

- Meeting Management provides a small subset of possible space settings.

  If you want to configure additional settings to space templates you have created using Meeting Management, then you can use the Meeting Server API. See the Cisco Meeting Server API Reference Guide.

- Templates that you have created or edited via the API will be visible in Meeting Management but you can only see the subset of the settings that can be edited in Meeting Management.
- Some settings in Meeting Management are a combination of multiple API settings.

  We have combined some settings to make it easier to configure templates.

- The settings you configure using Meeting Management will replace any existing settings when you commit them.

  This will only affect the specific settings that you configure. For instance, if you have defined a streaming URI for the space, this is not affected by settings you can configure from Meeting Management.

16.8.2 How to assign space templates to specific web app users

To create a space template:

1. Go to the **Servers** page and click **Set up provisioning**.
2. On the **Provisioning** page, **Allow users to create spaces** tab, click **Add Rule**.
3. Choose a **User import**.
4. Optional: Add a **Filter**.
5. From the **Chose space template** drop-down, choose an existing template, or **Create new template**.
6. If you chose an existing template, click **Done** and ignore the following steps.

   If you chose to create a new template, click **Create space template** and continue with the following steps.

7. Enter a space **Template name**.

   This is the template name that users will see in the web app when they choose which type of space to create.

   Note: If you use special characters in the template name, then they may appear differently in status messages, displaying escape characters instead. The name will still appear correctly in the web app.

   ---

8. Write a space **Template description**.

   This is the template description that users will see in the web app when they choose which type of space to create.

9. Decide if different roles should be differentiated by their passcode, or if they should each have a unique URI and Meeting ID.

   URI is called video address in the web app.

   Note: The Meeting Server recognizes roles by a participant's access method, which can be either the weblink or a unique combination of URI and passcode. The Meeting Server will add auto-generated passcodes if they are necessary to tell roles apart, or if you set a minimum password length. web app users can add or change passcodes when they manage their spaces.

10. Click **Add role**.
11. Enter a **Role name**.

    This is the participant role name that web app users see when they choose which invitation details to send to someone.

12. From the **Visibility** drop-down, choose the visibility scope for the template.
13. Enter a **Unique URI generator** to define a rule for how the Meeting Server should generate the URI that participants with this role should use to access the space.

    The URIs are created based on the space name, the URI generator, and the domain. For example, if you entered $.host, and a user creates a space called The A team on the domain example.com, then the URI would be ***`the.a.team.host@example.com`***

    Note: This field is disabled if you chose to use the same URI for all roles.

14. Decide if you want to override the system default for minimum passcode length.

    If you ignore this setting, Meeting Management will choose to use the system default.

15. If you chose to override the system default, enter a minimum passcode length.

    The default minimum length is 4 characters. If you do not want to require a passcode, then enter 0.

    Note: If you have chosen to use the same URI and numeric ID for all roles, and there is more than one role, then the Meeting Server will ignore that you have chosen 0.

16. Click **Next**.

17. Check the **Make this role an Activator** check box if you want participants with this role to be Activators.

    Activators can start meetings, and they can let other participants in from the lobby.

    If you are creating a host and guest space, we recommend that hosts are Activators and guests are non-Activators. If you are creating a team space where you want all participants to have the same role, then you should make them Activators.

18. Configure permissions for the role.

    *For each of the listed settings, you can check the **Override** check box if you want to override the settings that are configured for the default space call leg profile. The default call leg profile is defined by a combination of factory settings and settings defined via the API.*

    *To define a new setting, check the **Override** check box and choose the value that you want from the following options:*

    Table 9: Options available while configuring permissions for the role

Field name	Description
Maximum participants	Set a maximum number of active participants in the meeting.
Recording mode	Choose one of the following options: **Disable**: Recording is disabled **Manual**: Users can start and stop recordings **Automatic**: All meetings in the space are recorded
Locked by default	Set if all meetings in this space will start locked.
Passcode timeout (seconds)	Set the number of seconds the Meeting Server will wait for participants to enter a passcode when prompted before falling back to a role without passcode. To disable the timeout, enter a value of 0.
Video allowed	Set whether to allow participant video in meetings in this space. Sharing presentation video is always allowed, even for audio-only meetings.
Default video layout	Set the default video layout seen by participants in this meeting.
Behaviour when last activator leaves	The experience of remaining participants in the meeting when the last Activator leaves.
Allow change role	Participants with this permission can change role

19. Click **Next**.
20. Repeat adding more roles until you have added all the roles you want in this space template.
21. Use **Default for dial out** to select a default role for dial out participants during the meeting.

22. Click **Next**.
23. Define settings for the spaces that will be created from this template.

    *To use the system value for a setting, leave the **Override** check box unchecked.*

    *To define a new setting, check the **Override** check box and choose the value that you want.*

    Note: If you want to define other settings than listed here, then you can adjust the templates via the Meeting Server API. See the *Cisco Meeting Server API Reference Guide* for information.

24. Click **Done**.

Note: Your changes will not be applied before you have committed them. After you have committed the changes, template settings will take effect immediately. Changes to LDAP server details and any changes that affect users will take effect next time the Meeting Server is synchronized with the LDAP servers.

Note: All changes to provisioning settings that you have entered in Meeting Management will be lost if you restart Meeting Management before the changes have been committed.

16.9 Provisioning – Review and commit

The provisioning **Review and commit** tab will show provisioning settings.

If you have made changes that have not yet been committed, then the tab will show the settings that are local to Meeting Management.

- **Commit changes**: If you commit the changes, they will overwrite the current settings on the Meeting Server with the ones displayed here.

  Note: Your changes will not be applied before you have committed them. After you have committed the changes, template settings will take effect immediately. Changes to LDAP server details and any changes that affect users will take effect next time the Meeting Server is synchronized with the LDAP servers.

  Note: If you get the error message "Changes could not be committed at this time", some of the changes may have been committed. Check that all provisioning settings in Meeting Management are correct, and try again.

- **Discard changes**: If you discard the changes, then Meeting Management will retrieve the last committed settings from the Meeting Server and update the tab to show these.

If you have not configured any new settings, the tab will show the settings that Meeting Management has retrieved from the Meeting Server, and the buttons will be disabled. Settings are retrieved from the Meeting Server every 5 minutes, except while you are making changes to your settings.

16.10 Provisioning - LDAP sync

The last step of provisioning is to run an LDAP sync. This is required for the Meeting Server to import users from the LDAP server and apply the committed provisioning settings.

We also recommend that you perform an LDAP sync when there are changes to the information on the LDAP server, such as new users.

On the **Provisioning** page, **LDAP sync** tab, you can set up a regular sync schedule or manually trigger a sync, and you can see the status of recent syncs.

To configure scheduled syncs:

1. Click **View / edit sync schedule**.
2. To minimize disruption to active meetings, choose which Call Bridge should run the LDAP sync.
3. Choose on which days of the week the sync should run.
4. Choose at which time of day the sync should run, and click **OK**.

Note: The sync schedule is set on Meeting Management, and Meeting Management triggers each sync at the scheduled time. If you remove the Call Bridge the sync runs on, then scheduled syncs will not be run.

To manually trigger an LDAP sync:

1. Below the table, from the **Run a sync now on:** drop-down, choose which Call Bridge should run the LDAP sync.

   To minimize disruption to active meetings, choose the Call Bridge that hosts fewer or less important meetings than the other Call Bridges.

2. Click **Run sync now**.

Note: The Meeting Server will sync with all LDAP servers that are connected to it.

Note: Every time you change any provisioning settings, we strongly recommend that you check that your settings have been applied correctly. Meeting Management reports whether the sync was successful, but it cannot check whether the defined groups or mappings were implemented as you planned.

---

17 Logs – logs, crash reports, detailed tracing

As an administrator, you can access all logs for Meeting Management and Meeting Server.

Note: Most timestamps are in UTC. The exception is event logs which are displayed in your browser's time zone when viewed within Meeting Management.

Note: Event logs for a specific meeting are available on the **Meetings** page, meeting details view, for up to a week after the meeting has ended. See the *User Guide for Video Operators* for details. Event log information is also included in the Meeting Management system log, but you will not see the messages sorted by the meeting they belong to.

17.1 Meeting Management logs

All the Meeting Management logs including log bundle, system logs and audit logs can be accessed on the **CMM logs** tab.

17.1.1 Log bundle

From the **Logs** page **CMM logs** tab, you can download a log bundle for Meeting Management using **Download log bundle** button. The downloaded logs contain information that Cisco Support would need for troubleshooting:

- The latest system and audit logs
- Configuration details (redacted to not include passwords)
- Version number
- A list of crash reports
- 90 day license report
- Number of attempts or retries made for reserving licenses

If you need to contact Cisco Technical Support, always include the log bundle.

Note: All logs accessed on the **CMM logs** tab are for Meeting Management are for Meeting Management, even though many of the messages are based on information received from Meeting Server Call Bridges.

17.1.2 System log servers

On the **System log server** tab, you can add the servers to which Meeting Management should send the system logs. System logs contain all information on what has happened on Meeting

Management. The latest system logs are included in the log bundle. You can configure up to 5 system log servers to track events and activity on Meeting Management.

Only the latest logs are stored locally, so we strongly recommend that you set up an external syslog server to keep the full history in case you need it for Support.

Note: When troubleshooting issues with Meeting Management, you may need to look at Meeting Server logs as well. We strongly recommend that you use external syslog servers for all instances of Meeting Management, and for all your Meeting Servers.

To configure system log servers:

1. Click **Add log server** button
2. Enter **Server address** and **Port**
3. Select **Protocol**
4. Upload certificates using **Upload certificate** button
5. Click the **Add** button to complete configuring the log server

17.1.3 Audit log servers

On the **Audit log server** tab, you can add the servers to which Meeting Management should send the audit logs. Audit logs contain information about actions performed by Meeting Management users. For example, any settings change, login details and so on.

If audit logs are required in your organization, we recommend that you set up an external syslog server for audit logs. You can configure up to 5 system log servers to track events and activity on Meeting Management.

To configure audit log servers:

1. Click the **Add log server** button
2. Enter **Server address** and **Port**
3. Select **Protocol**
4. Upload certificates using the **Upload certificate** button
5. Click the **Add** button to complete configuring the log server

17.1.4 Crash reports

The Meeting Management crash reports can be accessed on the **Crash reports** tab in **CMM Logs** page

17.1.5 Detailed tracing

When requested from support, you can enable detailed tracing while reproducing an issue to gather comprehensive logs.

Detailed tracing is available for:

- Meeting Server API
- Meeting Server CDR
- Meeting Server Events
- TMS API
- Meeting Server Cloud Connector API

You can configure to trace logs for every 1 minute, 10 minutes, 30 minutes or 24 hours.

17.1.6 90 day license report

90 day license report provides visibility on customers' licensing usage to the support team, without having them to join a Webex meeting. The support team can then parse the 90 day license report and notify the customers of any necessary changes to the licenses.

17.2 Capture PCAP files in Meeting Management

From the **Logs** page **CMM logs** tab, you can navigate to **CMM PCAP** page and start capturing packets continuously to avoid delays while processing pcaps for trouble shooting networking issues in Meeting Management.

To capture pcap:

1. On the **CMM logs** tab, click **Start PCAP** button. The packets are captured in .zip file.
2. Download or delete PCAP file using the download or delete button respectively available against captured pcap file.
3. Click **Stop PCAP** button to stop packet capturing.

Once initiated, the packets are captured continuously unless the administrator stops packet capturing using Stop PCAP button.

Packets are captured in multiple files, on rotation. When a pcap file size exceeds 500MB, the packets are captured in a new file. This allows packet to be captured perpetually until the administrator stops. Meeting Management saves upto four pcap files with a total maximum file size limit of 2GB at any given time. Once the fourth pcap file size exceeds 500MB, the oldest pcap file is deleted.

17.3 Meeting Server logs

Meeting Management administrators can download log bundle and trace detailed logs for Meeting Server and Edge nodes using the **CMS logs** tab in the **Logs** page.

17.3.1 Log bundle

Meeting Management allows administrators to collect the logs for servers including Call Bridge and Edge Nodes after adding them.

The steps for collecting logs for Meeting Servers are as follows:

1. Click **Select server** button
2. Select Call Bridges or Edge Nodes from a list of servers
3. Click **Generate log bundle** button to generate the logs

Note: To generate log bundle for all the nodes in a cluster, on the Select Server page while selecting the cluster node, ensure that you select each node in the cluster.

After the log bundle is generated, you can download the logs of the selected server. The generated log bundle is named **logbundle_<host name>_YYYY-MM-hh-mm-ss.tar.gz**. The generated logs can be downloaded within 24 hours from the **CMS log bundle** page.

17.3.2 Detailed tracing

Meeting Management allows the administrators to trace logs of different Meeting Server modules like SIP, Active Control, Active Speaker, ICE and so on.

The steps for enabling detailed tracing are as follows:

1. Click **Select server** button
2. Select Call Bridges from a list of servers to trace the detailed logs.
3. In the **Traces** list, you can enable or disable tracing for different Meeting Server components.

Note: Enabling tracing debug is an overload on the selected servers. Ensure that you enable detailed tracing only when necessary.

You can also set how often you want to trace the logs. For example, you can configure to trace logs for every 10 or 60 minutes or you can set an interval of your choice in the hh:mm format.

Note: To generate log bundle for all the nodes in a cluster, on the Select Server page while selecting the cluster node, ensure that you select each node in the cluster.

Click **Disable all** to disable detailed tracing for all Meeting Server components.

17.4 Add or edit log servers

We strongly recommend that you set up at least one syslog server for system logs. This is required for our support team to be able to offer efficient support.

Note: The latest system logs are stored locally, but the limit is 500 MB of system logs. When the limit is reached, the oldest 100 MB of logs are deleted.

To add a system log server:

1. On the **Logs** page, choose **System log servers**.
2. Click **Add log server**.
3. Enter server address and port number.

   Default ports are:

   - *UDP: 514*
   - *TCP: 514*
   - *TLS: 6514*

   Note: If you type in IPv6 addresses, do not use square brackets here.

4. Choose protocol.
5. Optional: **Check certificates against certificate revocation lists (CRLs)** if you have chosen to use certificates, and you want Meeting Management to reject the connection if a certificate has been revoked.

   Meeting Management will block the connection if a certificate in the chain has been revoked, or if there is a CRL it cannot access.

   We recommend that you enable this when possible.

   Note: Only certificates with HTTP Certificate Distribution points (CDPs) are supported. If you are using CRL checks, and a certificate has no CDP, or if the CDP is not reachable via HTTP, then the connection is rejected.

   Also, your network must be configured so Meeting Management can connect to external address via HTTP.

6. If you chose TLS, **Upload certificate**.

   The requirements for the certificate chain are:

   - *It must include the full certificate chain, up to and including the root CA certificate.*
   - *The address listed in the certificate must be the same as the one you have entered for the log server.*

7. Click **Add**.
8. Repeat until you have added the log servers you need.
9. Restart Meeting Management

Optional: If required in your organization, add a syslog server for audit logs.

To add an audit log server:

1. On the **Logs** page, choose **Audit log servers**.
2. Click **Add log server**.
3. Enter server address and port number.

   Default ports are:

   - UDP: 514
   - TCP: 514
   - TLS: 6514

   Note: If you type in IPv6 addresses, do not use square brackets here.

   ---

4. Choose protocol.
5. Optional: **Check certificates against certificate revocation lists (CRLs)** if you have chosen to use certificates, and you want Meeting Management to reject the connection if a certificate has been revoked.

   Meeting Management will block the connection if a certificate in the chain has been revoked, or if there is a CRL it cannot access.

   We recommend that you enable this when possible.

   Note: Only certificates with HTTP Certificate Distribution points (CDPs) are supported. If you are using CRL checks, and a certificate has no CDP, or if the CDP is not reachable via HTTP, then the connection is rejected.

   Also, your network must be configured so Meeting Management can connect to external address via HTTP.

   ---

6. If you chose TLS, **Upload certificate**.

   The requirements for the certificate chain are:

   - *It must include the full certificate chain, up to and including the root CA certificate.*
   - *The address listed in the certificate must be the same as the one you have entered for the log server.*

7. Click **Add**.
8. Restart Meeting Management

18 Licenses

The **Licenses** page shows the following:

- A box displaying license status for each feature.

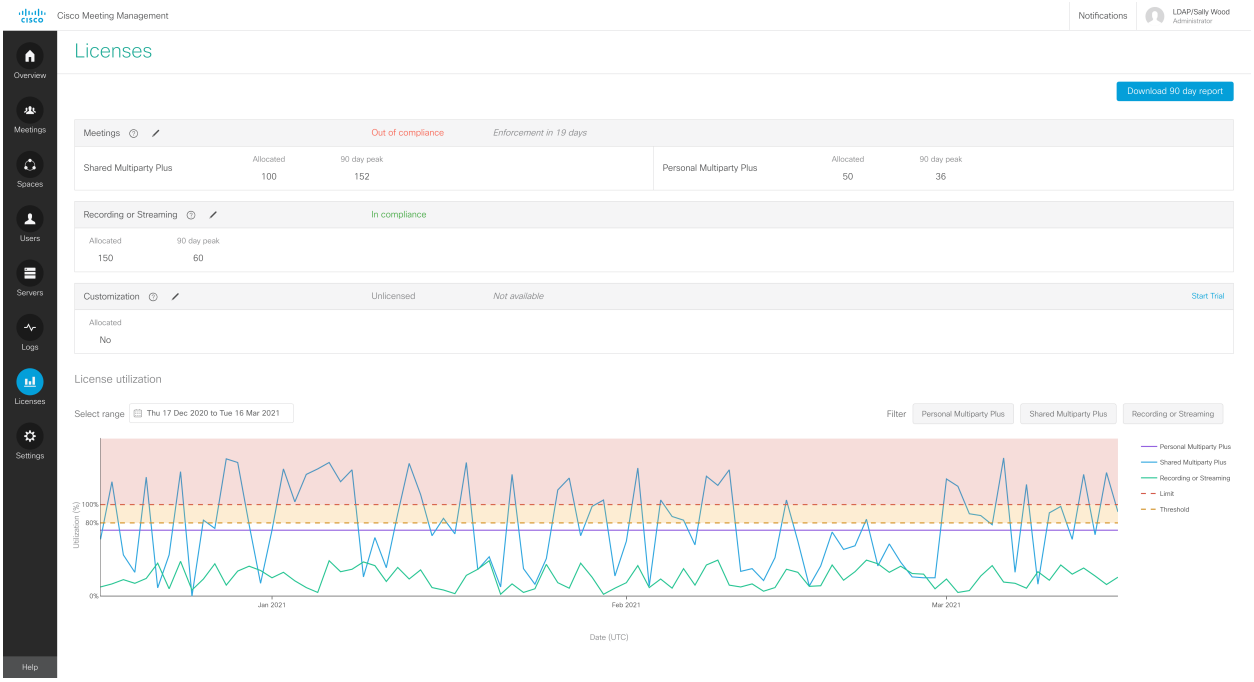
  See status definitions in License status and enforcement.

- Graphs of license utilization over time. You can specify a date range, and you can filter the graph based on license type.

> Note: For date ranges of one day, Meeting Management displays one data point per 5 minutes. For longer date ranges, there is one data point per day showing the peak value.

Meeting Management has deprecated the support for local license files (traditional licensing mode) and introduces License Reservation. In an environment where Meeting Management cannot connect to the Internet due to security reasons, License reservation can be used to activate features and reserve licenses. For more details, refer Licensing section.

The screenshot below shows the **Licenses** page in Smart Licensing mode.



For each feature, the box displays the following information:

- Box header: Name of feature, then license status, and then enforcement warning, if any. If you have not used your trial, then there will also be a **Start trial** button to the right.

  See the License status and enforcement section for more information.

- **Reserved**: The number of license reserved in Cisco SSM in case of SLR license reservation mode.
- **Allocated**: The number of available licenses

  For Smart Licensing, you enter the number, and Meeting Management verifies with the Cisco Smart Software Manager.

- **90 day peak**: Highest number of licenses used within the last 90 days

If you want more details than you can see in the summary, you can **download 90 day report**.

Meeting Management will provide a zip file named **license-data.zip**, which contains the following files:

- **host-reported.csv**

  This file contains the raw data as Meeting Management receives it from the separate Call Bridges in the cluster. Each row will display:

  - Host ID for the specific Call Bridge
  - Time stamp (UTC)
  - For each license type, number of licenses used.

- **cluster-bins.csv**

  This file contains cluster wide license use for each 5-minute interval, as calculated by Meeting Management. Each row will display:

  - Time stamp for start time of the 5-minute interval (UTC)
  - For each license type, summary of licenses used for all Call Bridges.

- **daily-peaks.csv**

  This file contains daily peaks, as calculated by Meeting Management. Each row will display:

  - Date (UTC)
  - For each license type, peak number of licenses used that day after 3 point median smoothing

19 License status and enforcement

If licensing is enabled in the instance of Meeting Management that you are signed in to, it keeps you up to date on the licensing status for your Cisco Meeting Server deployment.

Licenses are sorted by functionality:

- **Meetings**: This consists of activation of the Call Bridge and user licenses. If you have the appropriate licenses, then the Call Bridge can be used.

  For Smart Licensing: No activation key is required. If you have any PMP Plus or SMP Plus licenses available in your Virtual Account, then all connected Call Bridges can be used.

- **Recording or streaming**: These licenses allow recording or streaming.

  For Smart Licensing, recording and streaming is licensed when you have recording or streaming licenses available.

- **Customization**: This license allows customized layouts.

  For Smart Licensing, you can create customized layouts on the Meeting Server if you have a customization license.

The license status levels for Meetings are:

- **In compliance**: You have used 80% or less of the installed licenses.
- **Unlicensed**: You have not allocated any licenses.
- **Over 80% threshold**: You are still in compliance with your license agreement, but you have used more than 80% of the installed licenses.
- **Insufficient licenses**: You have used more licenses than available on 1–14 days within the last 90 days.

  We allow temporary overuse as you may have unexpected peaks. However, we recommend that you evaluate your usage data and consider if you need to purchase more licenses.

- **Out of compliance**: You have used more licenses than available on 15 days or more within the last 90 days.

  You are out of compliance with the license agreement. You should contact your Cisco partner or account team to discuss your needs and purchase more licenses.

The license status levels for Recording or streaming are:

- **Unlicensed**: You have not allocated any licenses for recording or streaming.
- **In compliance**: You have used 80% or less of the installed licenses.
- **Over 80% threshold**: You are still in compliance with your license agreement, but you have used more than 80% of the installed licenses.
- **Insufficient licenses**: You have used more licenses than available on 1–14 days within the last 90 days.

  We allow temporary overuse as you may have unexpected peaks. However, we recommend that you evaluate your usage data and consider if you need to purchase more licenses.
- **Out of compliance**: You have used more licenses than available on 15 days or more within the last 90 days.

  You are out of compliance with the license agreement. You should contact your Cisco partner or account team to discuss your needs and purchase more licenses.

The license status levels for customization are:

- **Licensed**: You have a customization license.
- **Unlicensed**: You do not have a customization license.
- **Out of compliance**: You have turned customization on in Meeting Management, but you do not have a customization license.

  *This is only seen for Smart Licensing. You are out of compliance with the license agreement. You should change the allocation to **No** or contact your Cisco partner or account team to discuss your needs and purchase a license.*

Note: Meeting Server APIs can also be used to fetch license status which includes, the feature components for a Meeting Server, each component's license status and expiry date. API object **`/clusterLicensing`** returns the license status and expiry date (if applicable) for a Meeting Server cluster. For more information, refer to Cisco Meeting Server API Reference Guide.

19.1 Available trials

There are three types of trial:

- **Meetings trial**: This trial gives you unlimited licensing of all features, including recording or streaming and customization, for a period of 90 days.

  You will not be offered a Meetings trial if Meetings is licensed, or if you have previously used your trial.

- Recording or streaming trial: This trial gives you unlimited use of recording and streaming for a period of 90 days.

  You will not be offered a recording or streaming trial if you already have recording or streaming licenses, or if you have previously used your trial.

- Customization trial: This trial allows you to use customized layouts for a period of 90 days.

  You will not be offered a customizations trial if you already have a customizations license, or if you have previously used your trial.

Note: You get one trial of each type per Meeting Management deployment, shared between all the connected clusters. You cannot get a new trial by moving a cluster to a new Meeting Management deployment, as Meeting Management will not offer a trial if any of the connected clusters have previously been connected to a Meeting Management instance during a trial of the same type. Also, you cannot get a new trial by adding a new cluster that was not connected during the first trial.

Note: If you do not add licenses before a trial ends, then you will be out of compliance, and enforcement will be active. See details in the table below.

19.2 License status during and after trial

Trial type	What is included in the trial	License status during trial	License status after trial
Meetings	Unlimited use of meetings, recording and streaming, and customized layouts for 90 days	In compliance	If you have any PMP Plus or SMP Plus licenses, then meetings will be in compliance. If you do not have any PMP Plus or SMP Plus licenses, then you will be unlicensed, and enforcement will be active until you add licenses. If you have any recording or streaming licenses, then recording or streaming will be in compliance. If you do not have any recording or streaming licenses, then recording or streaming will be unlicensed and unavailable. If you have a customization license, then customization will be licensed. If you do not have a customization license, then customization will be unlicensed and unavailable.
Recording or streaming	Unlimited recording and streaming for 90 days	In compliance	Recording or streaming will be in compliance if you have any recording or streaming licenses. If you do not have any recording or streaming licenses, then it will be unlicensed and unavailable.
Customization	Customized layouts for 90 days	Licensed	Customization will be licensed if you have a customization license. If you have no customization license, it will have the status unlicensed, and it will not be available.

19.3 Enforcement and warnings

On the **Licenses** page you can see both license statuses and warnings about upcoming enforcement.

Warnings and enforcement for meetings:

- **Enforcement in <number> days**: This is Alarm 1. You are out of compliance, and Meeting Management is counting down to enforcement.
- **Enforcement active, high enforcement in <number> days**: This is Alarm 2, which means that enforcement is active. Meeting participants will see and hear warnings at the beginning of each meeting.
- **High enforcement active**: This is Alarm 3, which means that the highest level of enforcement is active. Meeting participants will hear warnings at the beginning of each meeting, and they will see an on-screen warning in larger text during the whole meeting.

Warnings and enforcement for recording or streaming:

- **Available for <number> more days**: Meeting Management management counts down to enforcement.
- **Not available**: You cannot record or stream meetings.

Warnings and enforcement for customization:

- **Available for <number> more days**: Meeting Management management counts down to enforcement.
- **Not available**: You cannot use customized layouts.

20 Blast dial monitoring

Using blast dial monitoring, you can assign a primary or secondary role to your Meeting Management to avoid multiple dial outs when a space is accessed. This can happen when more than one Meeting Management monitors blast dial in a space.

- Primary – You must only set one Meeting Management to be Primary. This is the Meeting Management that will trigger blast dial under most circumstances.
- Secondary – This Meeting Management will attempt to trigger blast dial after a time delay. It will only do this if no other Meeting Management has started to dial out. The time delay can be configured in the field, Delay (seconds) when Secondary is chosen.
- Off – This Meeting Management will never trigger blast dial.

21 Settings – configure Meeting Management

On the **Settings** page, you can configure settings for Meeting Management, such as:

- Network settings for your Meeting Management
- The certificate that Meeting Management presents in incoming HTTPS connections.
- The CDR receiver address on which Meeting Management receives information from Call Bridges
- TMS settings
- NTP settings
- Sign in messages
- Advanced security

This is also where you can back up, restore, upgrade, and restart Meeting Management.

21.1 Edit network details

You have already set up basic network details, but you may want to add a DNS server or edit the configuration.

To edit network settings:

1. Go to the **Settings** page, **Network** tab.
2. Enter **FQDN**

   Note: Ensure that a fully qualified domain name (FQDN) is configured in the network settings. Using an incomplete FQDNmay result in login failures.

3. Enter **DNS servers**
4. Check on the option **Use IPv4**.

   If FQDN field is provided with a short name (hostname) before upgrading, Meeting Management can still be accessed via its IPv4 address, and the hostname can be updated to the FQDN afterward.

5. Check on the option **Use IPv6**.

   Note: If you type in IPv6 addresses, do not use square brackets here.

6. To save the details, **Restart** Meeting Management.

21.2 Upload certificate

When the Meeting Management certificate expires, you must replace it with a new one.

Note: Meeting Management does not have capabilities to create a certificate signing request. Use a separate tool, for instance OpenSSL toolkit, to create the private key and the certificate signing request.

To replace the certificate:

1. Go to the **Settings** page, **Certificate** tab.
2. **Upload certificate** to replace the expired certificate with a new one.
3. **Upload key**.
4. **Save** the details and **Restart** Meeting Management.

Certificate requirements:

- *The certificate chain should include the certificate of the CA that signed the certificate, plus any certificates higher in the certificate chain, up to and including the root CA certificate.*
- *Your CDR receiver address, as well as any addresses your users will use for the browser interface, should be included in the certificate.*

  Note: When the SAN field is used, Meeting Management does not look at the Common Name. The CDR receiver address must be included in the SAN field.

21.3 Edit CDR receiver address

The CDR receiver address is the address that Meeting Management will tell Call Bridges to send CDRs (call detail records) to. It is crucial that the CDR receiver address is set correctly for you to see meeting information in Meeting Management.

Note: We strongly recommend that you use an FQDN, as IP addresses may change. The CDR Receiver address field configures *only* what Meeting Management tells Call Bridges to use, not how your Meeting Management is presented to the wider network. You need to enter an address that is set up in your network to be resolvable and reachable from your Call Bridges.

To enter your CDR receiver address:

1. Go to the **Settings** page, **CDR** tab and enter your **CDR receiver address**.
2. Click **Save** and **Restart** Meeting Management.

21.4 Connect to TMS

To see scheduled meetings before they start, or to use TMS phonebooks to look up contacts when you add participants, you need to connect TMS to your Meeting Management.

Note: Before you can connect to TMS, your Call Bridges must be connected to the TMS booking API. For details, see the "Before you start" section of the *Installation and Configuration Guide*.

To connect Meeting Management to TMS:

1. Go to the **Settings** page, **TMS** tab.
2. Check the **Use TMS with Meeting Management** check box.
3. Enter IP address or FQDN for your TMS server.
4. Choose HTTP or HTTPS.
5. Optional: **Check certificates against certificate revocation lists (CRLs)** if you have chosen to use certificates, and you want Meeting Management to reject the connection if a certificate has been revoked.

   Meeting Management will block the connection if a certificate in the chain has been revoked, or if there is a CRL it cannot access.

   We recommend that you enable this when possible.

   Note: Only certificates with HTTP Certificate Distribution points (CDPs) are supported. If you are using CRL checks, and a certificate has no CDP, or if the CDP is not reachable via HTTP, then the connection is rejected.

   Also, your network must be configured so Meeting Management can connect to external address via HTTP.

6. If you are using HTTPS, upload certificate for your TMS.

   Certificate requirements are:

   - *The certificate should be a chain that includes the certificate of the CA that signed TMS certificate, plus any certificates higher in the certificate chain, up to and including the root CA certificate.*
   - *The server address you entered for your TMS server must be included in theTMS server certificate.*

     Note: When the SAN field is used, Meeting Management does not look at the Common Name. The TMS FQDN must be included in the SAN field.

7. Enter **Username** and **Password** for your TMS.
8. **Save** and **Restart** Meeting Management.

Note: You will not receive any information from TMS before you associate clusters with TMS.

21.4.1 Associate cluster with TMS

To tell Meeting Management which Call Bridge is connected to TMS and to enter its TMS System ID:

1. On the **Servers** page, click **Associate cluster with TMS**.
2. Select the Call Bridge that is the primary Call Bridge in TMS.
3. Enter the **TMS System ID**.
4. Click **Done** to start seeing scheduled meetings for the Call Bridge.

   Meeting Management will then verify the information and show the status **Associated with TMS** for the cluster, and the Call Bridge that is connected to TMS will get the label **TMS**.
5. Repeat until you have verified all clusters you want to see upcoming meetings for.

21.4.2 Get access to TMS phonebooks

Meeting Management can access TMS phonebooks so video operators can use them to look up contacts when they add participants to a meeting. The search will work the same way as it does when you search for contacts in TMS.

Note: TMS may support contacts that cannot be reached by your Meeting Servers. Make sure that you either update your outbound dial plans for the Meeting Servers or filter out phonebook entries the Meeting Servers cannot reach following the existing dial plan rules.

If a video operator tries to add a participant who cannot be reached from your Meeting Servers then Meeting Management will try to connect and fail. There will be no warnings or error messages. The video operator will see a spinner for a short while, and after that the participant will appear in the participant list as a disconnected participant.

Note: In TMS you can configure the number of search results to be displayed. This does not affect Meeting Management. Meeting Management always displays up to 50 search results.

To let your video operators use TMS phonebooks, you must go through three steps:

- Add Meeting Management as a phonebook client in TMS.

  We recommend that you edit your phonebooks first so it only includes contacts who can reached

- Assign phonebooks to your Meeting Management in TMS.
- Enable use of TMS phonebooks in Meeting Management.

Note: You need to connect Meeting Management to TMS before you can do this.

To add your Meeting Management as phonebook client in TMS:

1. In Meeting Management, go to the **Settings** page, **TMS** tab.
2. Copy the MAC address.
3. Sign in to TMS and go to **Phone Books**, then **Phone Book for Cisco Meeting Management**.

   *If you click the **Phonebook for Cisco Meeting Management** link in Meeting Management you will be taken directly to the correct view after you sign in to TMS.*
4. Click **New**.
5. In the Server Name field, enter a name for your Meeting Management.

   You can choose any name you want as long as it makes sense for other Meeting Management and TMS administrators.
6. In the MAC Address field, enter the address you copied from Meeting Management.

To assign phonebooks to your Meeting Management:

1. In TMS, go to **Phone Books**, then **Phone Book for Cisco Meeting Management**.
2. Click on the name you gave your Meeting Management in TMS.
3. Choose the phonebooks you want to use for your Meeting Management, then **Save**.

To start using the phonebooks:

1. In Meeting Management, go to the **Settings** page, **TMS** tab.
2. Check the **Use TMS phonebook** check box.
3. In the area above, enter the password for the account you used when you first connected Meeting Management to TMS, then **Save** and **Restart** Meeting Management.

21.5 See NTP status or add NTP servers

It is important that your Meeting Management is always synchronized with your Meeting Server Call Bridges, so we recommend that your Meeting Management uses the same NTP servers as your Meeting Server deployments. You can connect up to 5 NTP servers to Meeting Management, and you can monitor their status on the **Settings** page, **NTP** tab.

Note: The time displayed is for your Meeting Management server and may differ from the time settings on your computer.The offsets shown are between each connected NTP server and your Meeting Management server.

To add an NTP server:

1. Go to the **Settings** page, **NTP** tab.
2. **Add NTP server**.

   Note: If you type in IPv6 addresses, do not use square brackets here.

3. To save the changes, Restart your Meeting Management.

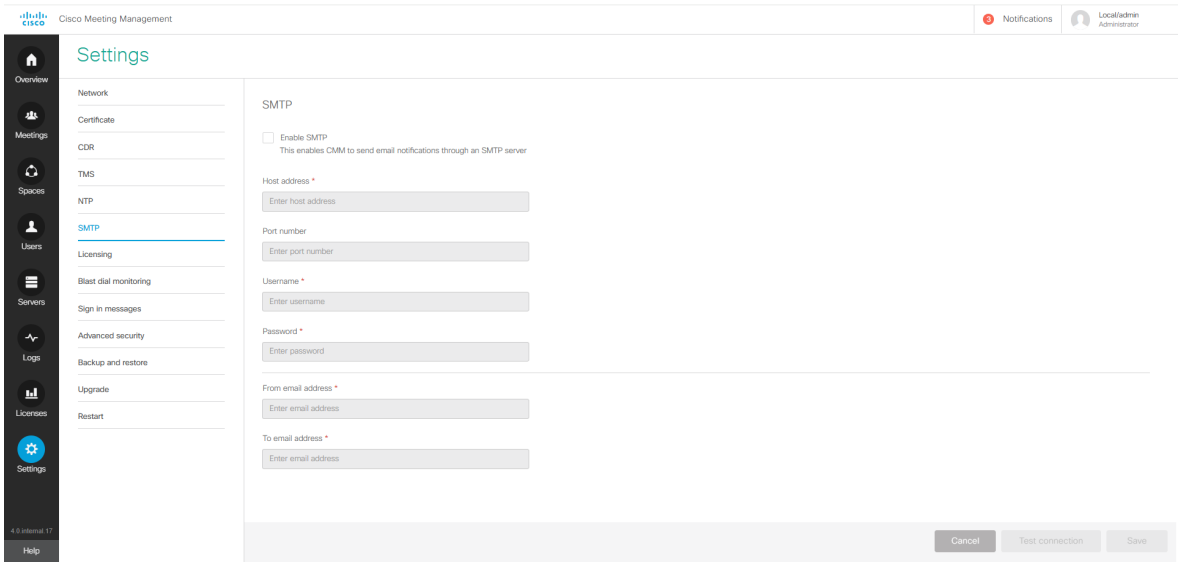
21.6 Add SMTP Servers

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

Enabling the **Enable SMTP** checkbox in the **SMTP** page of **Settings** tab allows the administrator to configure an SMTP server to send email notifications. To configure an outbound SMTP server, follow these steps:

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

5. Enter the destination email address where notifications will be sent in **To Email address**.



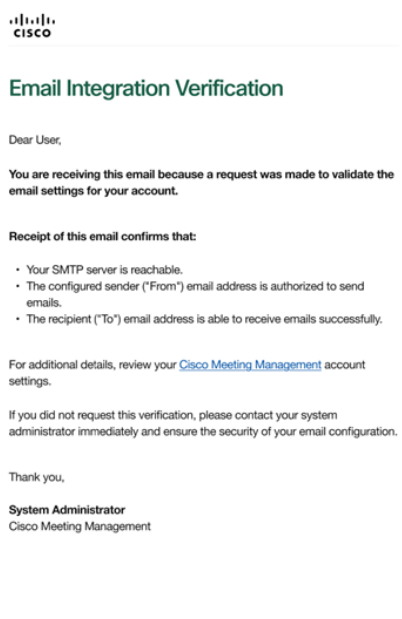
6. Click the **Cancel** button to reset the details you have entered.
7. Click **Test connection** to verify the server connection. A successful connection triggers a verification email, confirming the "From" address is authorized to send and the "To" address can receive email notifications.
8. Once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

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

Note:

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

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



Email Integration Verification

Dear User,

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

Receipt of this email confirms that:

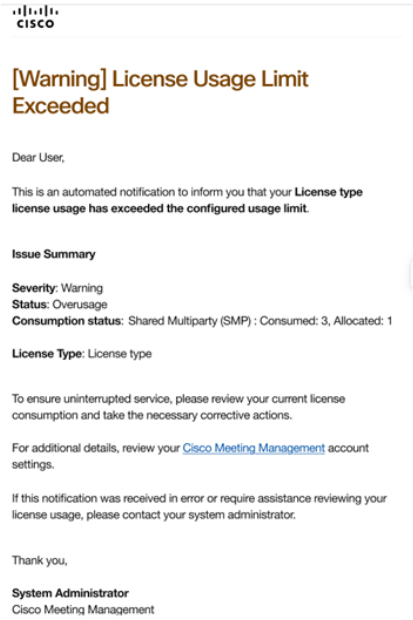
- Your SMTP server is reachable.
- The configured sender ("From") email address is authorized to send emails.
- The recipient ("To") email address is able to receive emails successfully.

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

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

Thank you,

System Administrator
Cisco Meeting Management



[Warning] License Usage Limit Exceeded

Dear User,

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

Issue Summary

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

License Type: License type

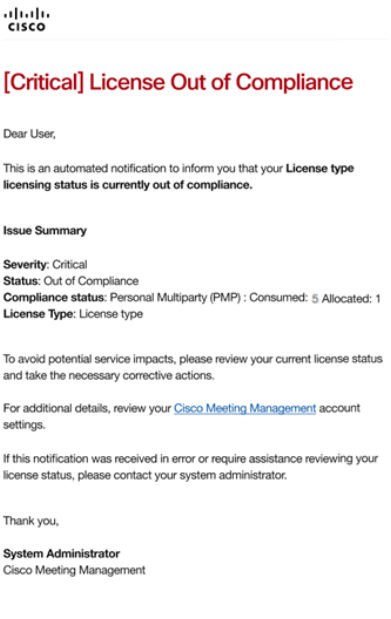
To ensure uninterrupted service, please review your current license consumption and take the necessary corrective actions.

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

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

Thank you,

System Administrator
Cisco Meeting Management



[Critical] License Out of Compliance

Dear User,

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

Issue Summary

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

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

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

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

Thank you,

System Administrator
Cisco Meeting Management

The email notifications will be triggered once in case:

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

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

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

21.7 Licensing

On the Settings page, Licensing tab, you can choose the licensing mode. If you have chosen Smart Licensing, you can also configure some of the Smart Licensing settings here.

You must choose a licensing mode. Choose between:

- **Smart Licensing** (recommended)

  Your license status may show as out of compliance until you register with the Cisco Smart Software Manager and set your license allocations.

  When you choose Smart Licensing, then Meeting Management gets information about purchased licenses from the Cisco SSM.

  Note: There is no CLI (command line interface) for the Meeting ManagementSmart Licensing integration. This is by design as Meeting Management provides a graphical user interface.

- **You no longer need to have activation keys installed on the connected Call Bridges**. Instead, Meeting Management reports the number of Call Bridges without a traditional license key to the Cisco Smart Software Manager. They appear as a license type called **Active Call Bridge Node** in your Smart Account. These licenses are free, and you will automatically be given the number of licenses you need.
- **No licensing**

  This option is only for resilient deployments. Choose this option if you have a resilient deployment, and you have enabled either Smart Licensing on the other instance of Meeting Management.

Note:

- The **Traditional Licensing** option is grayed out for users who were using this licensing mode in previous versions of Meeting Management.
- Meeting Management has deprecated the support for local license files (traditional licensing mode). Traditional Licensing option is no longer available in **Licensing Mode** pop-up once you migrate to Smart Licensing.
- After you change licensing mode or add a new cluster, it may take up to 5 minutes before the changes affect the license status for connected Meeting Servers.

21.7.1 How to enable Smart Licensing

To enable Smart Licensing:

1. Sign in to the Cisco SSM and generate a registration token.

   Note: While generating the registration token, ensure that you select **Allow export-controlled functionality on the products registered with this token** option to enable higher levels of product encryption functionality. For more information, refer Smart Software Manager On-Prem User Guide

2. Copy the token to your clipboard.
3. Open the instance of Meeting Management that you want to use for license reporting.
4. Go to the **Settings** page, **Licensing** tab.
5. Click **Change**.
6. Choose **Smart Licensing** and **Save**.
7. Click the **Register** button.
8. Paste the registration token.
9. Optional: Register this product instance if it is already registered

   Usually Cisco SSM will not let you register an instance of Meeting Management that is already registered. If you check this check box, then Cisco SSM will let you register the same instance again. This is useful if your Meeting Management has lost the registration details, for instance if you have tried to deregister and Meeting Management could not reach Cisco Smart Software Manager while deregistering.
10. Click **Register**.
11. When you have registered, check how many licenses you have in your Virtual Account.
12. In Meeting Management, go to the **Licenses** page.
13. Enter information about the licenses you have in your Virtual Account.

    Note:

    - If you want to test Meeting Management and don't yet have licenses, then you can click **Start trial** instead.
    - If you do not have any licenses of a specific type, enter 0 rather than leaving the field blank.

Note: After you update the licensing mode or add a new cluster, it may take while before Meeting Management has fetched all the usage information to update the license status. This can take from a few minutes to over 15 minutes, depending on the speed of your connection and the volume of data.

Note: Every time you change the number of allocated licenses, it may take up to 5 minutes before the changes affect the license status for connected Meeting Servers.

Note: While reserving a license, if Cisco SSM takes more time than the expected 30 seconds to respond, two more retries will be attempted with varying timeout values. Meeting Management waits for 60 seconds and 90 seconds for second and third retry respectively. If license reservation is unsuccessful after three retries, **Overview** page displays **Unable to reach Cisco Smart Software Server**. Reserving license will have to be reinitiated and the message will be cleared ones the licenses are successfully reserved.

21.7.2 Smart Licensing actions after Smart Licensing has been enabled

You can do the following:

- **Renew Authorization Now**: The system automatically renews your authorization daily, at midnight UTC. However, if you want to renew manually, you can do that here. This is useful if you have purchased new licenses or allocated more licenses to the Virtual Account for this Meeting Management, and you want to see the changes in Meeting Management immediately.
- **Renew Registration Now**: The system automatically renews your registration every 6 months. You may want to renew the registration manually if you have moved licenses to or from the Virtual Account for this Meeting Management, or if you have moved this instance of Meeting Management to a different Virtual Account.
- **Reregister**: You can reregister manually if you want to use different Virtual Account with this instance of Meeting Management.
- **Reserve Licenses**: Smart Licensing enables you to activate and manage licenses using your Smart Account. You can activate a product instance by generating a token in Cisco Smart Software Manager and reserve licenses required for the product instance. Smart Account ensures that the selected product instance is in compliance and is authorized with enough licenses to support the current license requirement across all devices. For more information check this section.
- **Deregister**: You can deregister this instance of Meeting Management if you want to use the Virtual Account for another deployment, or if you have a resilient Meeting Management deployment and want to use the other instance for reporting.

  Note: If you change the licensing mode, then Meeting Management will automatically disable Smart Licensing and deregister from the Cisco Smart Software Manager.

  Note: If you have lost connection to an instance of Meeting Managementthen you can also deregister from the Cisco SSM.

21.7.3 License Reservation

To be compliant with SMART, Cisco product users require support for License Reservation. Meeting Management supports license reservation from version 3.4 onwards. In an

environment where Meeting Management cannot connect to the Internet due to security reasons, License reservation can be used to activate features and reserve licenses.

The feature has two variants: Universal (Permanent License Reservation) and Specific (Specific License Reservation).

- **Universal variant**: Universal or Permanent License Reservation (PLR) provides a single license that enables use of all features in the product. PLR is only available for Military/Defense customers.
- **Specific variant**: Specific License Reservation (SLR) provides you with a choice to reserve licenses based on your requirement. In addition to feature licenses, user licenses such as SMP Plus and PMP Plus can also be reserved. If license usage changes, this feature allows updating or changing the license reservation.

License reservation can be changed from Universal to Specific variant and vice versa. This involves returning the reservation and re-registering the product instance.

Note: The license reservation feature is not enabled on customer Smart Accounts by default and must be specifically requested by the customer and approved by Cisco. Both types of License Reservation require Cisco to authorize the Smart Account. You must have a Smart Account for your company with a dedicated Virtual Account that will be used by only one instance of Meeting Management. To request an account, talk to your Cisco account team or go to Cisco Software Central.

License reservation allows the following workflows:

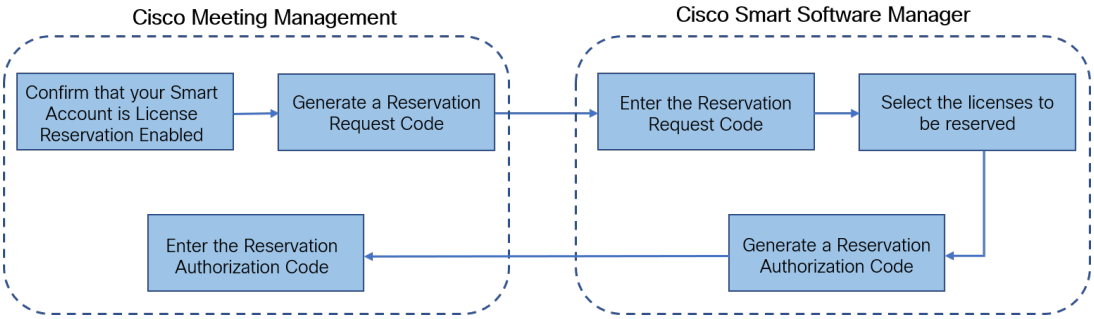
- Reserve SLR/PLR licenses
- Update reserved licenses
- Return reserved licenses

21.7.3.1 License Reservation

The workflow for initial license reservation is as follows:

1. Confirm that the Smart Account is License Reservation enabled
2. Generate a Reservation request code from Meeting Management
3. Enter the code in Cisco SSM
4. In case of SLR, select license to be reserved
5. Generate a Reservation Authorization Code in Cisco SSM
6. Enter the authorization code in Meeting Management

Figure 3: Workflow for License Reservation



Follow these steps for license reservation:

1. In Meeting Management **Settings**, go to the **Licensing** section:
    a. Click the **Register** button to open **Smart Software Licensing Registration** pop-up.
    b. Click the **start here** link at the bottom of the pop-up to initiate the license reservation process.
    c. In the pop-up window that opens, click **Yes, My Smart Account is License Reservation Enabled**.
    d. In the **Smart License Reservation** pop-up, click **Generate** button to generate Reservation Request Code.
    e. Save or copy the Reservation Request Code that is generated.
    f. Click **Close**. In **Smart Software Licensing** page of Meeting Management, the **Smart Software Licensing Status** will be displayed as **License Reservation Pending**.

2. In Smart Software Manager
    a. Log in to Cisco Smart Software Licensing Manager using your Smart Account
    b. Navigate to the desired Virtual Account and click **License Reservation**

    Note: Use of license reservation requires specific permission from Cisco. For this, user has to make sure **License Reservation** button is available in**Licenses** tab under **Inventory** section of Smart Software Manager.

    c. Enter the Reservation Request Code.
    d. Choose licensing from **Licenses to Reserve**:
        - For PLR - Select option **Meeting Server PLR Enablement**
        - For SLR - Select option **Reserve a specific license** and select the specific licenses to be reserved.

        Note:
        The LIC-CMS-ENCRYPT-S license is highly recommended for all customers to enable encryption on Meeting Server call bridges. Encryption licenses are required per deployment; ensure that sufficient licenses are purchased to cover all the Meeting Management instances.

    e. Click **Generate Authorization Code** button to generate the Reservation Authorization Code.
    f. Save or copy the Reservation Authorization Code.

    Note: In case of Specific licensing, on selecting **Reserve a specific license** in **Licenses to Reserve**, user can view a list of available licenses. Ensure to select enough quantity of licenses while requesting in the Smart Account.

3. In Meeting Management, perform the following steps:
    a. In **Smart Software Licensing** page, open **Enter Reservation Authorization Code** pop-up.
    b. You also have an option to view reservation request code or cancel Reservation Request
    c. Enter the Reservation Authorization Code generated from Smart Software Manager and click **Install Authorization Code/File** button to complete reservation.
4. In the **Licensing** section, the **Registration** status under **Smart Software Licensing Status** will change:
    - from **License Reservation Pending** to **Registered - License Reservation**
    - and **License authorization** as **Authorized - Reserved**.
5. The license status in the **Licenses** page will be displayed as:
    - **Reservation Active** for PLR
    - **Reserved** along with the number of licenses for SLR.

21.7.3.2 Update reserved licenses

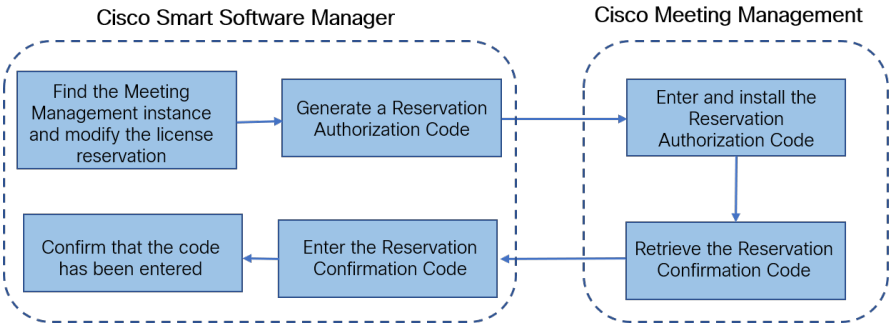
To meet the changing needs of your organization, you can update specific licenses or you can change the number of reserved licenses. For example, your current license requirement is 5 and you want to add another 5 licenses, then you need to select the number of licenses as 10 and the new value overrides the prior value.

Note: Updating licenses is not applicable in case you are using PLR. However, you can change your license reservation type from PLR to SLR or vice versa. To change the type of license reservation, return the reserved licenses, unregister the product instance, and reregister the product instance from scratch. When changing your reservation from PLR to SLR, the selected licenses in SLR will override PLR licenses.

The workflow for updating reserved license is as follows:

1. Find the license instance to be updated in Cisco SSM
2. Generate a Reservation authorization code
3. Enter and install the code in Meeting Management
4. Generate a Reservation confirmation code
5. Enter and confirm that the Reservation confirmation code in Cisco SSM

Figure 4: Workflow for Update License Reservation



Follow these steps to update the reserved licenses:

1. In Smart Software Manager:
    a. Find Cisco Meeting Management instance from the **Product Instances** and select **Update License Reservation** from the **Actions** menu.
    b. Use the **Update License Reservation** pop-up to modify the licenses to be reserved and generate a new Reservation Authorization Code.
    c. Save or copy the Reservation Authorization Code.
2. In Meeting Management **Settings**,
    a. Navigate to the **Licensing** section and click on **Update Reservation** button.
    b. Enter the Reservation Authorization Code in the pop-up that gets open on clicking **Update Reservation** button.

    Note: In case the Meeting Management instance has reserved a Universal license, to update license reservation, return this license using **Return Reserved Licenses** button in **Licensing** section and then reregister the product instance.

    ---

    c. Click **Install Authorization Code** button to update license reservation and to generate a Reservation Confirmation Code.
    d. Copy or save the Reservation Confirmation Code by clicking **View confirmation code** button in **Smart Software Licensing** page.

3. In Cisco Smart Software Manager,
    a. Find Cisco Meeting Management instance in **Product Instances** and select **Enter Confirmation Code...** from the **Actions** menu to launch the **Enter Confirmation Code** pop-up.
    b. Enter the Reservation Confirmation Code into the **Enter Confirmation Code** pop-up.
    c. Return to the **Smart Software Licensing** page in Meeting Management and click **Code Has Been Entered** button to dismiss the alert that was placed after the Reservation Authorization Code was installed.

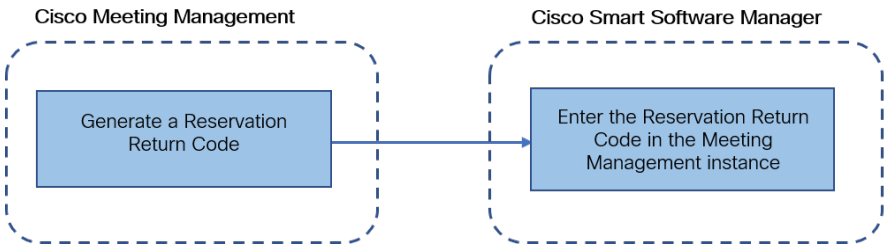
21.7.3.3 Returning reserved licenses

You can return the reserved licenses to theVirtual Account so that the licenses can be used by other product instances. To return licenses, follow the steps described in this section.

The workflow for returning a reserved license is as follows:

1. Generate a Reservation return code
2. Find the Meeting Management instances in Cisco SSM
3. Enter the Reservation return code

Figure 5: Workflow for Returning License Reservation



Follow these steps to return reserved license:

1. In the **Licensing** section of Meeting Management **Settings**,
    a. Click **Return Reserved Licenses...** button to launch the **Confirm Return Licenses** pop-up.
    b. Click **Generate** button to generate a Reservation Return Code.
    c. The **License Reservation Return Code** pop-up provides instructional text and allows to copy or download a file containing the License Reservation Return Code.

2. In Smart Software Manager,
    a. Find the Meeting Management instance in **Product Instances**
    b. Select **Remove** from the **Actions** menu to launch the **Remove Product Instance** pop-up.
    c. Enter the Reservation Return Code into the pop-up to complete returning reserved licenses. The **Registration** status is changes to **Deregistered** in the **Licensing** page.

21.7.3.4 Things to consider while migrating to Smart license

1. Existing traditional licensing files (PAK files) can be used for upgrading to 3.4 version.
2. Customers with existing licensing files (partially or fully fulfilled PAK) will need reference to originally purchased PAK to convert PAK license to Smart Licensing. You will have to open a new Global Licensing Org (GLO) request for manual conversion to Smart Licensing by providing the Smart Account name, domain, and virtual account in use.

    Note:
    • Self-service for converting PAK to Smart Licensing using Cisco SSM is only available for new customers.
    • Converting existing licenses to Smart license must be done with help of GLO team and might cause delay.

    ---

3. You should plan to convert your licenses to Smart Licensing a few days before upgrading to 3.4 version to prevent the requirement of using the one-time 90 day trial mode.
4. Ensure that your Smart Licensing Virtual Account has enough licenses for Meeting Server usage in last 90 days. In cases of overuse, Meeting Management will enter high enforcement alarm mode on conversion to Smart Licensing. If you are in high enforcement alarm mode, Meeting Management allows one time 90 day trial to silence alarm, giving time for you to purchase additional licenses.
5. Virtual edition CMS activation licenses (LIC-CMS-K9) cannot be converted to Smart Licensing, instead Cisco SSM automatically counts the number of Call Bridges in use and reports it under **Call Bridge Active Nodes** on the Smart Account. Customers will only be able to view the number of Call Bridges in use and cannot add new Call Bridges licenses.

21.8 Cisco Meeting Server Cloud Connector

Note: If you disable the service from Meeting Management, you only stop sending information from Meeting Management to the Webex Cloud. To fully deregister Meeting Management and disable the service, go to WebexControl Hub.

Cisco Meeting Server Cloud Connector is a hybrid service that lets you connect Meeting Management deployments to the Webex Control Hub and the Webex Cloud.

The service lets you:

- See information about Meeting Management instances in the Control Hub interface.
- Set up email and Webex Teams alerts, so you can get notified about Meeting Management errors and warnings.

The service also sends metrics to the Webex Cloud.

21.8.1 Cisco Meeting Server Cloud Connector status

You can see the following status information on the Cisco Meeting Server Cloud Connector tab:

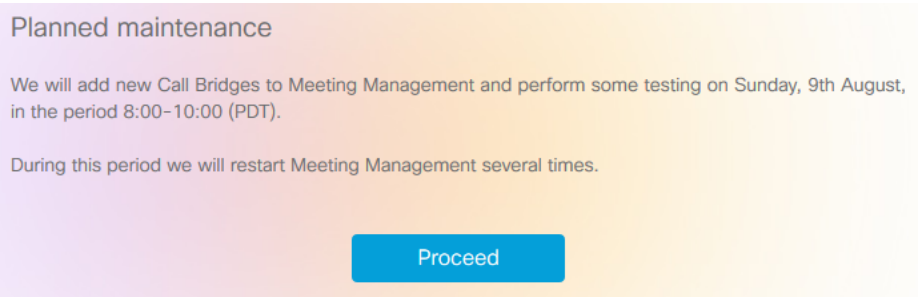
- Registration: This tells you if this instance of Meeting Management is registered to the Webex Cloud.
- Addresses of Webex Cloud services: This tells you which addresses Meeting Management needs to reach for Cisco Meeting Server Cloud Connector to work.

For detailed instructions and information see the Cloud Connector online help.

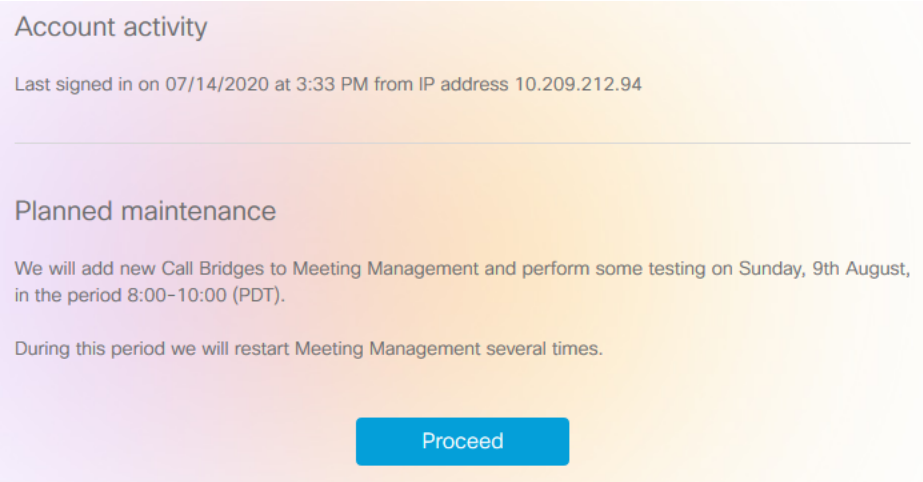
21.9 Display messages when users sign in

You can insert a page with a message for your users before or after the sign-in page. For example, you can use the pre-sign-in message for a legal warning and the post-sign-in message to notify them of planned maintenance.

The page will display the message you type in, and a **Proceed** button like the example below.



If you check the **Display account activity after sign-in** check box, the account activity will appear after sign-in. The screenshot below shows an example where both the account activity and a post-sign-in message are displayed.



Note: The changes will take place immediately.

21.10 Configure advanced security settings

On the settings page, **Advanced security** tab, you can configure advanced security settings. The default settings keep your Meeting Management functional and secure, so they are appropriate for most environments. We recommend that you only change the advanced security settings if your organization's local security policies require specific settings.

Note: All security settings require a restart before they are applied. If you set up advanced security settings as part of the first time setup, you can finish configuring all settings on the **Settings** and **Logs** pages before you restart.

21.10.1 Rate limit sign-in attempts

You can limit how many times users can attempt to sign in within a given interval. If you enable rate limiting, the settings configured here take effect for both LDAP users and local users.

The number of allowed sign-in attempts is measured in tokens. Each user starts with a maximum number of tokens that you have defined. They lose one token for each failed sign-in attempt, and they gain one at the end of each interval until they again have the maximum number of tokens available.

There are two settings:

- **Rate at which one token is added to a bucket (in seconds)**

  This is the length of each interval, measured in seconds. The default is 300 seconds.

- **The maximum numbers of tokens held in a bucket**

  This is the maximum number of sign-in attempts a user can be allowed within a given interval. The default is 3 tokens.

That means if users spend all tokens during the first interval, then they only get one attempt to sign in during the second interval. If users try to sign in after they have used up all their tokens, then they receive the message **Too many sign in attempts. Please try again later**. This happens even if the credentials are correct.

If the administrator has not configured rate limiting, Meeting Management by default allows a maximum of 20 failed sign-in attempts for both LDAP and local users, after which a lockout period of 15 minutes is enforced. If users attempt to sign-in after exhausting their retry attempts, they will receive the message: **Too many incorrect sign in attempts. Please try again later.** If a local user is locked out, an administrator can manually unlock the account by clicking the button available next to each local user in the local users list, found in **Users** > **Local**. However, the list will not indicate any status whether a local user is locked out or not. For LDAP users, the lockout cannot be bypassed until the default 15-minute lockout timer expires.

21.10.2 Idle session timeout

You can configure Meeting Management to sign out users who are inactive for a certain period of time. Meeting Management defines users as active when they move the mouse, click buttons, or enter text in input fields.

When you enable idle session timeout, the default timeout is 3600 seconds (one hour). The minimum is 60 seconds, and the maximum is 86400 seconds (24 hours).

Note: Meeting Management checks the status every 30 seconds which means that the timeout can be the set time limit plus up to 30 seconds.

Note: Even when you enable idle session timeout, users will still be signed out 24 hours after they signed in, whether they are active or not.

21.10.3 Reset meeting server password

You can reset the Meeting Server passwords used by Meeting Management to authenticate to Meeting Server, without validating the previous password. If the user has forgotten the password, they have the option to reset the password without validating the previous password. If this option is enabled, the user will not be prompted to enter the previous password, while resetting the password using the **Reset password** button in the **Edit Call Bridge** page (See Add Configured Server section).

Note: We strongly recommend using a dedicated administrator account for Meeting Management. We do not recommend using an API account for this connection.

The following setting is displayed:

Reset password without validating the previous password – Check this checkbox to enable password reset without validating the previous password. This option is unchecked by default.

21.10.4 TLS settings

You can choose which TLS cipher suites to enable for connections to and from Meeting Management.

The settings configured here take effect for all TLS connections, so it affects how Meeting Management connects to the following:

- Browsers
- LDAP server
- Call Bridges
- System log servers

- Audit log servers
- TMS
- Cisco Smart Software Manager

All connected browsers and servers support a range of cipher suites. If a connected unit supports more than one of the cipher suites that are enabled in Meeting Management, then Meeting Management will use the one that is closest to the top of the list.

By default, the following cipher suite is disabled:

- AES256-SHA

CAUTION: If you disable all cipher suites that are supported by a specific browser or server, then it can no longer be connected to Meeting Management.

Be particularly careful checking that you have cipher suites enabled that are supported by your preferred browser and your LDAP server. If your browser cannot connect to Meeting Management, or Meeting Management cannot connect to your LDAP server, then you may be locked out of Meeting Management.

21.11 Backup and restore

We recommend that you always create a new backup before you make any changes to Meeting Management. The backup contains:

- Configuration:
  - All details from the **Settings** page other than the licensing settings
  - LDAP server details
  - Details for all LDAP groups
  - Security policy settings for local users

    This includes settings for the passphrase generator, but not the dictionary
- Database:
  - Details for local users, including hashes of recent passwords
  - Details for all Call Bridges, including any TMS System IDs
  - Passphrase dictionary

21.11.1 Create a backup

We recommend that you create a backup before you start using your Meeting Management. Then you can easily re-use settings if you need to re-deploy.

1. If a restart is required, do this now so all settings can take effect.
2. On the **Settings** page, go to the **Backup and restore** tab.
3. Click **Download backup file**.
4. Enter a password, then **Download**.
5. Save the backup file and the password in a secure location.

   Note: The backup is encrypted and cannot be used without the password.

21.11.2 Restore a backup

Before you restore a backup:

- Make sure that you have your backup file and the password ready.

  The password was chosen when you or another administrator created the backup.
- Decide if you want to restore all settings, or if you just want to restore either database or configuration details (see step 4 below).
- Make sure that your LDAP server is online while you restore the backup.
- If you have TMS connected, make sure TMS is online while you restore the backup.

Note: If your LDAP server or TMS is offline while you restore, then the restore will fail.

Note: If you restore LDAP details, we recommend that you sign in as a local administrator to restore the backup.

To restore a previously saved backup:

1. On the **Settings** page, go to the **Backup and restore** tab.
2. Click **Upload backup file**.
3. **Select backup file**.
4. Choose one or both options:
    - **Restore configuration**:
        - All details from the **Settings** page other than the licensing settings
        - LDAP server details
        - Details for all LDAP groups
        - Security policy settings for local users

          This includes settings for the passphrase generator, passphrase verifier, enforce password complexity and enforce password expiration, but not the dictionary file.
    - **Restore database**:
        - Details for local users, including hashes of recent passwords
        - Details for all Call Bridges, including any TMS System IDs
        - Passphrase dictionary

    You will not be able to restore a backup if you do not check either of the two options.
5. Enter password, then **Restore**.

Note:

- If you are signed as a local user when you restore Meeting Management, then Meeting Management will add your account to the list from the backup, or it will update the backed-up profile with the current settings. All other settings will be replaced with the settings from the backup.
- On changing the password for administrator and video operator after taking the backup, then restoring the downloaded backup file, video operators can log in to Meeting Management using the restored password and administrators will be able to log in using the changed credentials.

21.12 Upload keys to validate upgrade images

Cisco Meeting Management embeds a signature within the upgrade image that verifies whether the image is genuine or tampered.

Image signatures are only verified when upgrading from a signed image. So manual verification is still advised when upgrading from an unsigned image to a signed image. i.e. if you upgrade

from 3.6 to 3.7, or downgrade to earlier versions, you are still advised to manually verify the hashes. This feature will be fully effective when upgrading from 3.7 and beyond.

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

To upload public keys:

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

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

21.13 Restart Meeting Management

Most settings in Meeting Management require a restart before they are applied.

To restart Meeting Management:

1. Go to the **Settings** page, **Restart** tab.
2. Click **Restart**.

Note: When you restart Meeting Management, all users are signed out without warning, and all information about meetings is deleted from Meeting Management. Start times for meetings that are still active after restart, as well as join times for participants who are still connected, will be restored via API requests. The times displayed in the meeting details will be correct, but entries in the event log will be given new timestamps.

Appendix A Security hardening

Security Hardening Information on how to deploy and operate VMware products in a secure manner is available from the VMware Security Hardening Guides.

Accessibility Notice

Cisco is committed to designing and delivering accessible products and technologies.

The Voluntary Product Accessibility Template (VPAT) for Cisco Master Project is available here:

http://www.cisco.com/web/about/responsibility/accessibility/legal_regulatory/vpats.html#telepresence

You can find more information about accessibility here:

www.cisco.com/web/about/responsibility/accessibility/index.html

B Accessibility support features

B.1 Keyboard navigation

You can use your keyboard to navigate through Meeting Management.

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

B.2 Screen reader support

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

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

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

Cisco Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

© 2026 Cisco Systems, Inc. All rights reserved.

Cisco Trademark

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