Cisco Meeting Management

Cisco Meeting Management 2.9

User Guide for Administrators

April 30, 2020

Cisco Systems, Inc. www.cisco.com

Contents

1 Introduction

This guide is for administrators of Meeting Management.

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

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

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

1.1 What is new in 2.9

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

1.1.1 Changes to this guide since 2.8

We have added the following sections:

- Provisioning
- Provisioning - LDAP servers
- Provisioning - Import users
- Provisioning - Allow users to create spaces
- Provisioning - Review and commit
- Provisioning - Run LDAP sync

We have made changes to the following sections:

- Deployment overview: Added a section on provisioning users and creating templates.
- Configure advanced security settings: Added a section on Idle session timeout. Also, we have removed some cipher suites that are no longer available.
- Servers: Added links to Associate cluster with TMS and Provisioning.

1.2 The software

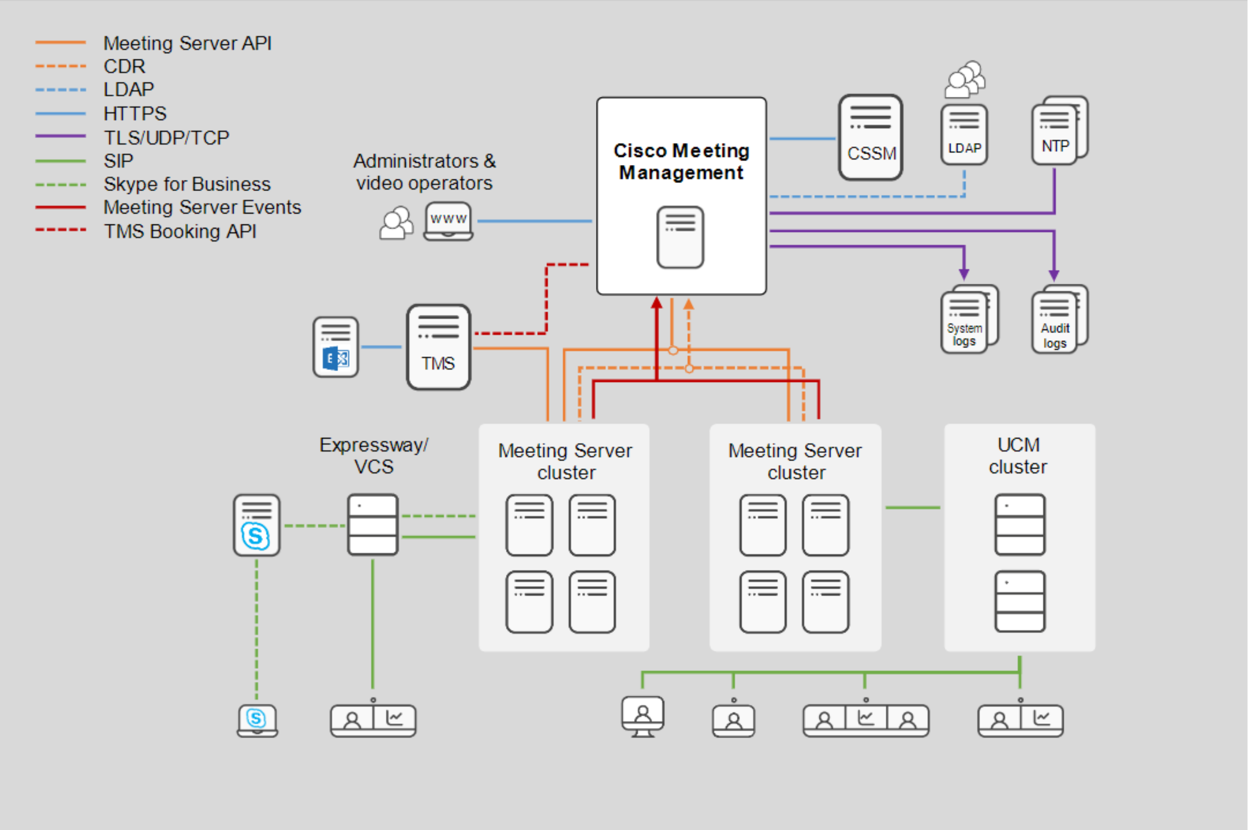
Meeting Management is a virtualized appliance. Specifications of the VM (virtual machine) depend on how many simultaneous actions your Meeting Management has to perform or observe. See the *Installation and Configuration Guide* for specifications and requirements, including our estimates on sizing related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

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

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. 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.

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 have at least one local administrator user account. This is to make sure that you can still access Meeting Management if there are LDAP issues. For general use in production we recommend that users are authenticated via LDAP.

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 it updates information about scheduled meetings every 5 minutes. 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 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. For traditional licensing, license files are installed on Call Bridges within the Meeting Server deployments, and Meeting Management receives information about both installed licenses and usage from the Call Bridges.

For Smart Licensing, 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.

2.6 Provisioning users and creating space templates on Meeting Server clusters

You can use Meeting Management to provision Cisco Meeting Server web app and Meeting App users 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.

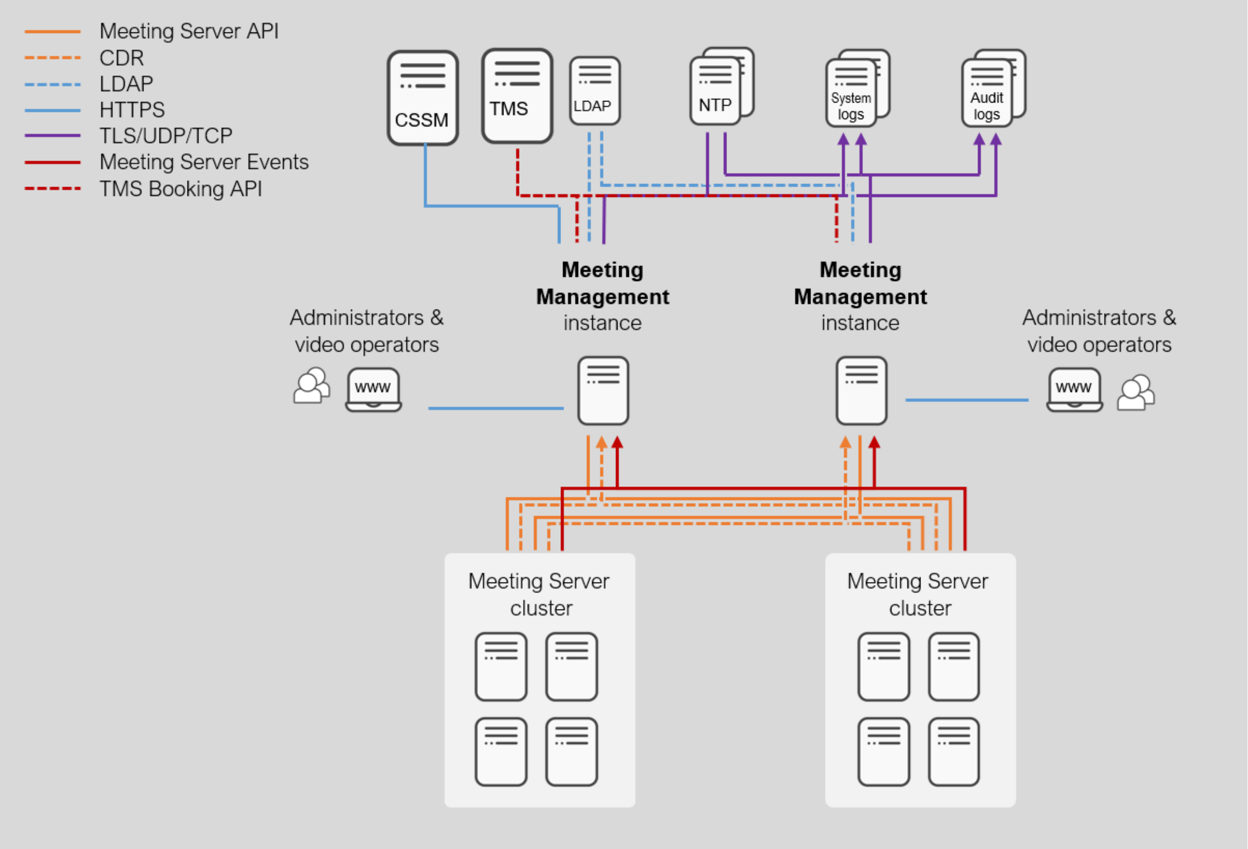
Note: For security and auditing reasons, we recommend that you create a separate bind user account for each Meeting Server cluster on each LDAP server.

2.7 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.

Figure 2: A resilient Meeting Management deployment



2.8 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.

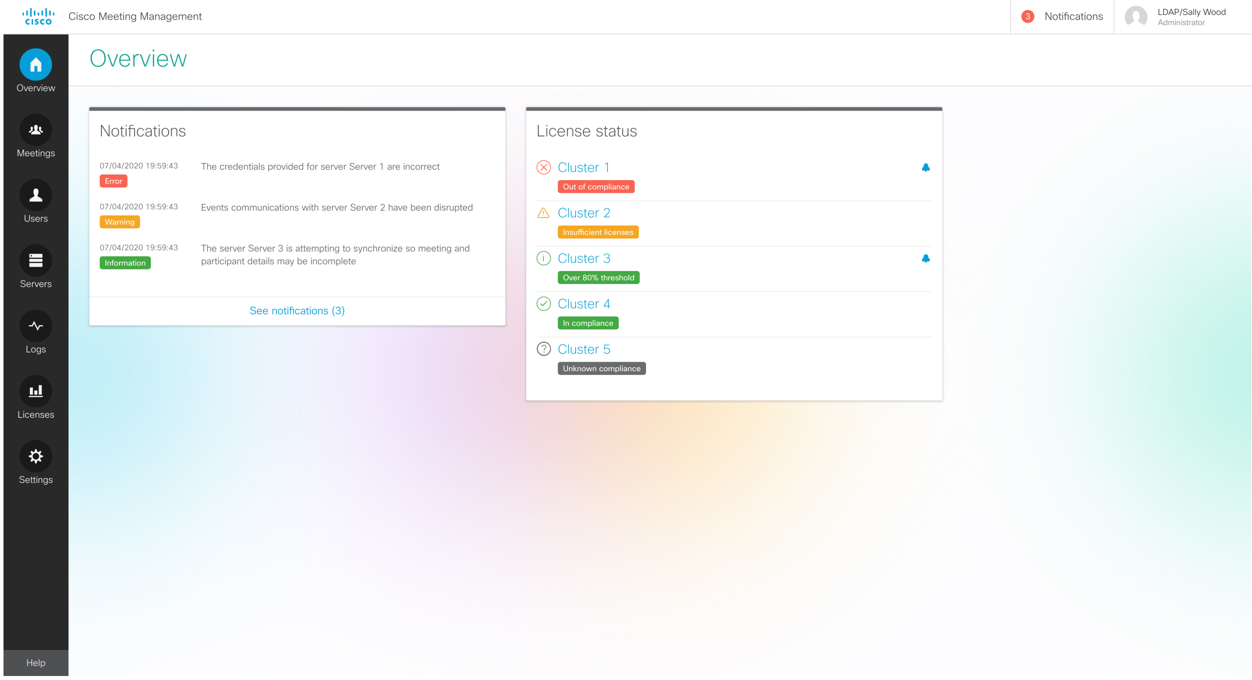
3 Overview - view notifications and license status

On the **Overview** page you can see system notifications and license 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



Overview

Notifications

07/04/2020 19:59:43 Error — The credentials provided for server Server 1 are incorrect

07/04/2020 19:59:43 Warning — Events communications with server Server 2 have been disrupted

07/04/2020 19:59:43 Information — The server Server 3 is attempting to synchronize so meeting and participant details may be incomplete

See notifications (3)

License status

Cluster 1 — Out of compliance

Cluster 2 — Insufficient licenses

Cluster 3 — Over 80% threshold

Cluster 4 — In compliance

Cluster 5 — Unknown compliance

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

You can also see status for license utilization on connected Cisco Meeting Server clusters.

There are 6 different status levels:

- **Out of compliance**: You have been out of compliance with your license agreement for more than 15 days.

  You get this warning if you have been over the limit for 15 or more days in a 90 day period. You should purchase more licenses.

- **Insufficient licenses**: You have temporarily used more licenses than you have installed, and you are out of compliance with your license agreement.

  You get this warning if you have been over the limit at any time within the last 90 days. You should purchase more licenses.

- **Over 80% threshold**: You are still in compliance with your license agreement, but you have used more than 80% of the installed licenses.
- **In compliance**: You have used 80% or less of the installed licenses.
- **Unknown compliance**: License status for clusters that have Cisco Meeting Server Capacity Units installed. Meeting Management cannot track Meeting Server Capacity Units.

The blue bell icon is displayed for a cluster if a new status update has not been marked as acknowledged by an administrator.

To see more details, click on a cluster name. This will open the **Licenses** page. This page shows further information about licenses and also displays any event log messages related to licensing that requires immediate action.

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 Users - Add users or edit user settings

5.1 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 have at least one local administrator user account. This is to make sure that you can still access Meeting Management if there are LDAP issues. For general use in production we recommend that users are authenticated via LDAP.

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.
- **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.

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.

5.2 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.

5.3 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.

5.3.1 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 **Next**.

8. 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.

9. Click **Done**.

10. Restart Meeting Management

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

5.4 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:

- Require a minimum password length

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

- 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.*

- 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.

5.5 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**.

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.

6 Servers - add or edit Call Bridges

On the **Servers** page you can see and edit all your connected Meeting Server Call Bridges. You can also add new Call Bridges, or you can edit details for a cluster. 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 use has already 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 any information about ongoing meetings.

To add a Call Bridge:

1. On the **Servers** page, click **Add Call Bridge**.
2. In the **Server address** field, enter the IP address or FQDN (fully qualified domain name) for your Call Bridge API.

   This is the same as your Web Admin Interface address.

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

3. In the **Port** field, enter the port number for your Call Bridge API.
4. Enter the **Username** and **Password** for your Call Bridge API.

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

5. 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.

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

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

8. 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 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.

9. Click **Add**.
10. Optional: **Rename cluster** to give it a name that makes sense to you as well as all other users.

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

To add auto-discovered Call Bridges:

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

To edit a Call Bridge:

1. Scroll down to the Call Bridge you want to edit and click ✎ or click anywhere in the row.
2. Edit details.
3. Click **Done**

7 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.

7.1 What do we mean by provisioning users?

Provisioning users means setting up user accounts for everyone who you want to use the Cisco Meeting App or the Cisco Meeting Server web app. This is done by importing users from one or more connected LDAP servers and defining some basic settings, such as:

- Which details should be used as username and display name
- Whether they are assigned a PMP Plus (Personal Multiparty plus) license
- Which types of spaces they can create

7.2 What is a space?

A space is a virtual meeting room that participants can dial into to have audio or video meetings. It may also serve as a chat room if chat is enabled on the Meeting Server. 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 Meeting App user guides and the visual "how to" guides. as well as the Important Information documents.

7.3 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.

7.4 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. Optional: Create space templates that users can use to create spaces.
5. Review and commit your settings.
6. Start an LDAP sync to perform the provisioning.

8 Provisioning – Before you start

8.1 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.

8.2 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 Server and 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.

8.3 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 app and Meeting App users 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.

9 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.

9.1 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.

   Note: These fields are case sensitive.

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 user imports 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.

10 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.

10.1 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 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 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. From the drop-down, choose the LDAP server you want to set this user import filter for.
4. 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.

   Note: This field is case sensitive.

5. 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.

6. Enter **Login user name mapping**.

   This defines which LDAP attribute you want to use as the username that Meeting Server web app and Meeting App users 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: This field is case sensitive.

7. Enter **Display name mapping**.

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

8. 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 user imports 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.

11 Provisioning - Allow users to create spaces

As part of provisioning you can create space templates that Cisco Meeting Server web app users can use to create new spaces.

On the **Provisioning** page, **Allow users to create spaces** tab, you can create space templates, which will be available to all the users you have set up imports for on the **Import users** tab.

11.1 Limitations

- You cannot use the templates to provision spaces for your users. The templates can only be used by the web app users to create their own spaces.
- You cannot define which users get to use which space templates.

  If you want to make different templates available to different users, then use the API to create and assign templates.
- 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.

  Note: Members can only be added using the Meeting App.
- 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.
- 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 API. See the "Create and apply coSpace templates" section of the the Meeting Server 2.9 Release Notes for instructions.
- 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.

- Sync error details are only stored in the Meeting Server system logs, and Meeting Management does not retrieve information about whether an LDAP sync has succeeded.

11.2 How to add a space template

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 space template**.
3. 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.

4. 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.

   Note: Meeting Management lets you enter more characters than you can commit to the Meeting Server. The limit for the Meeting Server is 200 bytes, which corresponds to up to 200 Roman characters with no accents, or around 50 Chinese characters.

5. 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 Meeting App and 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. Meeting Management will only add auto-generated passcodes if they are necessary to tell roles apart. web app users can add or change passcodes when they manage their spaces.

   Note: If you are using Meeting Management version 2.9.0 and you want to change from using unique URIs to all participants having the same URI after you have saved the space template, then you must remove all roles and create new ones for the change to take effect.

6. Click **Add role**.
7. 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.

8. Enter a **Unique URI generator** to define a rule for how the URI for the space is generated.

   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.

9. Click **Next**.
10. 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.

11. 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.*

    Note: The web app has some limitations. For example, no participants can add others to a meeting or control streaming when they dial in using the web app no matter what permissions they have. See all limitations in the *Cisco Meeting Server web app 2.9 Important information* document.

12. Click **Next**.
13. Repeat adding more roles until you have added all the roles you want in this space template.

    Note: All roles will be available in the web app. In the Meeting App, only one of these roles will be available in the invitation details, and no settings in Meeting Management can decide which role that will be.

    To define which role should be used for the invitation in the Meeting App, you can use the Meeting Server API to set the **scope** field to **public** for the role that should be used for invitations sent from the Meeting App. See "Multiple coSpace Access Methods" in the *Cisco Meeting Server API Reference Guide*.

14. Click **Next**.
15. 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 *Meeting Server 2.9 Release Notes* for information.

16. 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 user imports 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.

Note: Meeting Management lets you enter more characters than you can commit to the Meeting Server. The Meeting Server limit is 200 bytes, which corresponds to up to 200 Roman characters with no accents, or around 50 Chinese characters.

12 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: When you commit your settings, they are saved to the Meeting Server. Template changes take effect immediately. Changes to user imports take effect next time the Meeting Server is synchronized with the LDAP servers.

  Note: but no changes to users or space templates will be made before 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 are correct, and try again.

- **Discard changes**: If you discard the changes, then the settings that were last committed to the Meeting Server will be valid, and the tab will be updated 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.

13 Provisioning - Run LDAP sync

The last step of provisioning is to run an LDAP sync. On the Provisioning page, LDAP sync tab, you can manually trigger an LDAP sync so the cluster can perform the provisioning based on the settings you have configured.

To run an LDAP sync:

1. To minimize disruption to active meetings, choose which Call Bridge should run the LDAP sync.
2. Click **Sync now**.

Note: You cannot use Meeting Management to set up scheduled LDAP sync. However, you can use a cron job to send daily API commands to trigger LDAP sync. You can see an example script in the FAQ article How do I set up daily LDAP sync?.

14 Logs - logs, crash reports, detailed tracing

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

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

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 neatly sorted by the meeting they belong to.

14.1 Log bundle

From the **Logs** page, **Log bundle** tab, you can download a log bundle that contains 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

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

14.2 System logs

System logs contain all information on what has happened on Meeting Management. The latest system logs are included in the log bundle.

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.

14.3 Audit logs

Audit logs contain information about actions performed by Meeting Management users.

If audit logs are required in your organization, we recommend that you set up an external syslog server for audit logs.

14.4 Crash reports

From the **Logs** page, **Crash reports** tab, you can download or delete crash reports.

14.5 Detailed tracing

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

14.6 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

15 Licenses - view summary and events

On the **Licenses** page you can see a summary of license information and a history of related events.

A banner appears at the top of the page if the selected cluster has the status **Insufficient licenses** or **Out of compliance**. See the license status levels in Overview - see notifications.

15.1 Summary

The **Summary** tab shows the following:

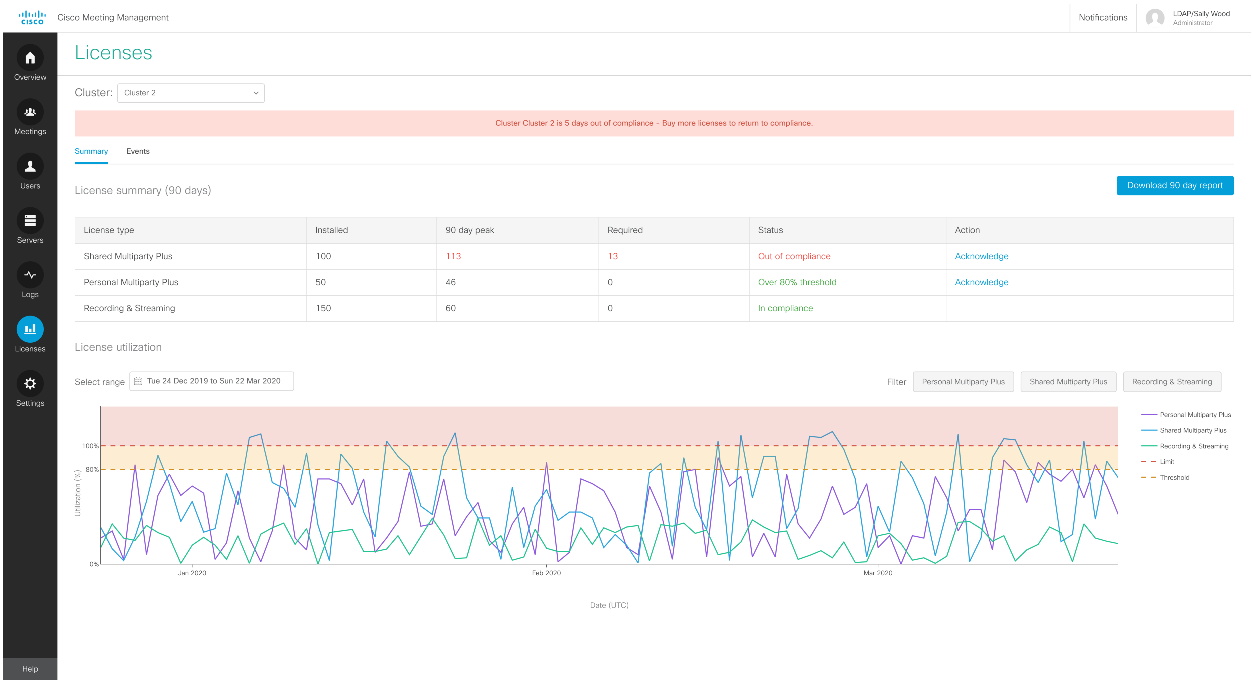
- A table displaying license status for each license type
- Graphs of license utilization over time. You can specify a date range, and you can filter the graph based on license type.

  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.

  Note: If you are using license of a type that has not been installed, no percentage can be calculated, and any utilization will be shown at the top of a broken y-axis.

Note: Meeting Management does not support license status for Capacity Units. The number of installed Capacity Units will appear in the table, but the use of Capacity Units will not be displayed anywhere.

In the 90 day report you can see the number of Capacity Units installed, but the use of licenses will be reported as if you were using SMP Plus or PMP Plus licenses.



Licenses

Cluster: Cluster 2

Cluster Cluster 2 is 5 days out of compliance - Buy more licenses to return to compliance.

License summary (90 days)

License type	Installed	90 day peak	Required	Status	Action
Shared Multiparty Plus	100	113	13	Out of compliance	Acknowledge
Personal Multiparty Plus	50	46	0	Over 80% threshold	Acknowledge
Recording & Streaming	150	60	0	In compliance	

License utilization

Select range: Tue 24 Dec 2019 to Sun 22 Mar 2020

For each license type, the table displays the following information:

- **Installed**: Number of licenses installed

  This is only seen for traditional licensing.

  Note: If you are using Smart Licensing, then the column header will say **Available for reporting**, and you must enter the number of assigned licenses manually, see Enable Smart Licensing.

  This is only seen for Smart Licensing.

- **Available for reporting**: Number of licenses allocated to this Meeting Management deployment, entered manually by you or another administrator.

  This is only seen for Smart Licensing.

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

- **Required**: Suggestion of how many licenses to purchase, based on the difference between installed licenses and the 90 day peak value

  This is only seen for traditional licensing.

- Last reported: The last peak that was reported to the Cisco Smart Software Manager.

  This is only seen for traditional licensing.

  Note: **90 day peak** is rounded up to nearest 1 decimal place, and the **Last reported** is rounded up to the nearest whole number. This means that in some cases, the number for **Last reported** may be higher than the number for **90 day peak**.

- **Status**: The status of compliance

  For an explanation of each status for traditional licenses, see Overview - see notifications and license status. For an explanation of the status for Smart Licensing, see embedded help on the **Settings** page, **Smart Software Licensing** tab.

- **Action**: If the status is **Over 80% threshold** or **Out of compliance**, an **Acknowledge** button is displayed here until you or another user clicks it.

  *When you click the **Acknowledge** button, you are verifying that you have seen the status and taken action as required in your organization. When you acknowledge the status, the button will disappear, the blue bell icon on the **Overview** page will show fewer unacknowledged statuses or disappear, and the **Events** will show all users that you have acknowledged the status.*

  Note: The **Acknowledge** button will reappear next time the daily peak is over the threshold.

The license status is based on status for the following license types:

- Personal Multiparty plus licenses

  These are assigned to specific users, and one license is valid for one active meeting.

- Shared Multiparty plus licenses

  These are shared between all users, and one license is valid for one active video meeting. Some meeting types consume only 1/6 of a license.

- Recording and streaming licenses

  These are shared between all users, and one license is valid for one ongoing recording or one ongoing streaming session.

See the *Cisco Meeting Server 2.6 Release Notes* as well as the *Cisco Meeting Server Deployment Guides* for more information on license types and how licenses are applied to meetings.

Note: If Capacity Units are installed, the table will display a row for those. It will only show how many units are installed; Meeting Management cannot track the use of these.

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.

  Note: Call Bridges report recording and streaming use separately, but Meeting Management tracks all recording and streaming together because they consume the same license type.

  Note: If Capacity Units are installed, the number of installed licenses will be displayed in the 90 day report, but the use of licenses will be shown as if you were using SMP Plus or PMP Plus licenses.

- **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**

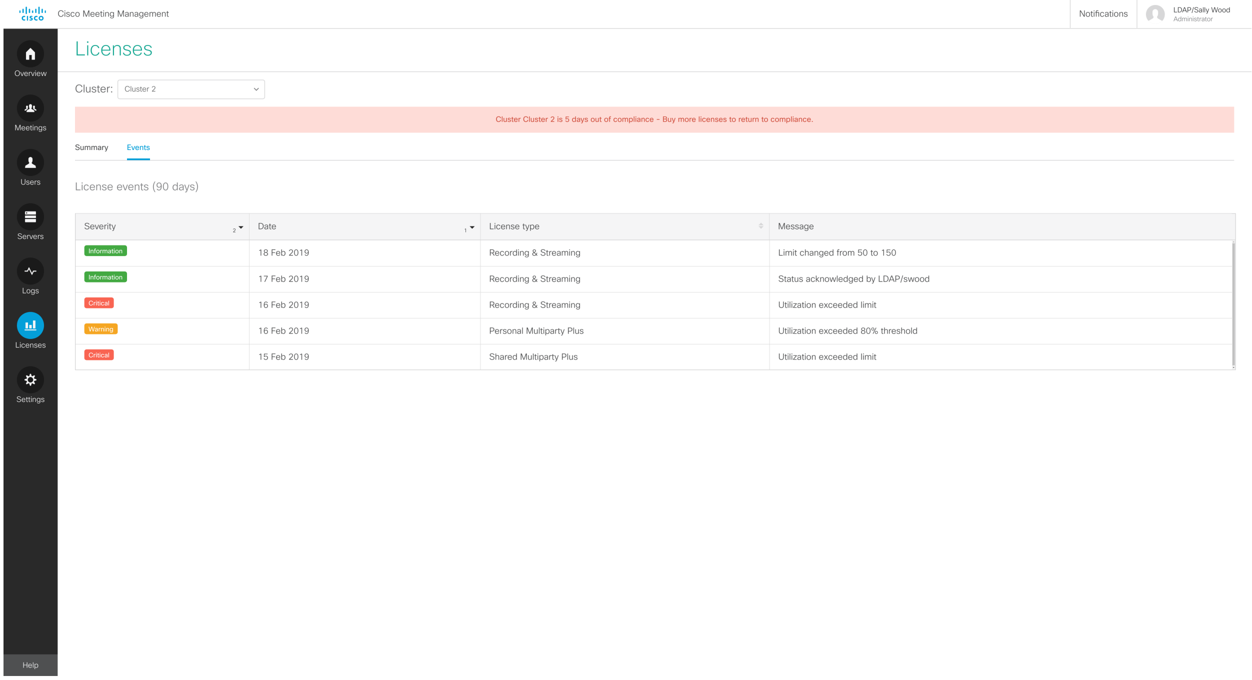
  This file contains daily peaks, as calculated by Meeting Management. Each row will display:

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

15.2 Events

The **Events** tab shows event log messages related to licenses.

You can click anywhere in the heading to sort the alerts by **Severity**, **Date** or **License type**.



Licenses

Cluster: Cluster 2

Cluster Cluster 2 is 5 days out of compliance - Buy more licenses to return to compliance.

License events (90 days)

Severity	Date	License type	Message
Information	18 Feb 2019	Recording & Streaming	Limit changed from 50 to 150
Information	17 Feb 2019	Recording & Streaming	Status acknowledged by LDAP/swood
Critical	16 Feb 2019	Recording & Streaming	Utilization exceeded limit
Warning	16 Feb 2019	Personal Multiparty Plus	Utilization exceeded 80% threshold
Critical	15 Feb 2019	Shared Multiparty Plus	Utilization exceeded limit

16 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.

16.1 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 the relevant details.

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

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

16.2 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.*

16.3 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.

16.4 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.*

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.

16.4.1 Associate cluster with TMS

To tell Meeting Management which Call Bridge is connected to TMS, and 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.

16.4.2 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.

16.5 See NTP status or add NTP servers

It is important that your Meeting Management is always synchronized with your Meeting ServerCall 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.

16.6 Smart Licensing

You can choose to use traditional licenses that are installed on the Meeting Server deployment, or you can enable Smart Licensing and manage all your licenses via the Cisco Smart Software

Manager.

Before you enable Smart Licensing, consider the following:

- **You must set up a Smart Account** if you do not already have one.

  To set up a Smart Account, go to software.cisco.com, then in the ***Administration*** *area click* ***Request a Smart Account****.*

- **Optional: Set up a separate Virtual Account for your Meeting Management licenses**.

  One Meeting Management deployment can be registered to one Virtual Account. You can have licenses for other products in the same Virtual Account, but you can only have licenses for one specific Meeting Server deployment in one Virtual Account.

- **Optional: Set up one Meeting Management deployment for each Meeting Server cluster**.

  All licenses are accumulated for the clusters that are connected to your Meeting Management deployment. If you want to keep licenses separate for different clusters, then each cluster must be connected to a separate Meeting Management deployment, and each of these Meeting Management deployments must be connected to a separate Virtual Account.

- **If you have set up a resilient Meeting Management deployment, decide which instance of Meeting Management you want to use for license reporting**.

  If you register both instances with Smart Licensing, then the Cisco SSM will receive the same license utilization reports twice for the same cluster, and it will determine that you are of compliance when you have used only half of the allocated licenses.

- **Determine how Meeting Management should connect to Cisco SSM**.

  If you need to set up a Proxy, or you are using Smart Software Manager On-prem (satellite), then you must have address, port number, and certificate available so you can ***Edit Transport Settings****.*

  For information on transport settings, see the Smart Licensing information page.

Also, note that there are some limitations:

- Reservation of licenses is not supported by Meeting Management.
- There is no CLI (command line interface) for the Meeting Management Smart Licensing integration. This is by design as Meeting Management provides a graphical user interface.
- Smart Licensing lets you know if you are in compliance or not. Unlike the traditional license reporting, it does not differentiate between short peaks and long term overuse.
- Smart Licensing does not report back to Meeting Management how many licenses have been allocated to the Virtual Account it is using. You must enter the number of licenses manually to see utilization in percentage.

- Smart Licensing does not work if at least one connected Meeting Server cluster is running Meeting Server version 2.5 or older.
- In this release, Smart Licensing works only for usage licenses (Recording, Streaming, SMP Plus, PMP Plus). You still need traditional activation licenses installed for a Meeting Server deployment to work.
- Smart Licensing cannot activate your deployment for evaluation. You must install traditional license (activation keys) for the Meeting Server deployment to work.

To enable Smart Licensing:

1. Sign in to the Cisco SSM and generate a registration token.
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, **Smart Software Licensing** tab.
5. Click **Enable**.

   Note: Evaluation mode is not implemented for this release, so you cannot use Smart Licensing to activate your Meeting Servers. You must install traditional licenses on the Meeting Servers for them to work. Evaluation mode will still work in the sense that Meeting Management does not send usage information to the Cisco Smart Software Manager while the deployment is in evaluation mode.

6. Click the **Register** button.
7. Paste the registration token.
8. 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.

9. Click **Register**.

To see utilization data on the **Licenses** page:

1. In the **License summary** table, enter the number of licenses allocated for this cluster in the **Available for reporting** column.

   Note: This is for you to see more details than what will be available in the Cisco Smart Software Manager. The details that you see in Meeting Management are not reported back to the Cisco SSM.

16.6.1 Actions after you have registered

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.
- **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.

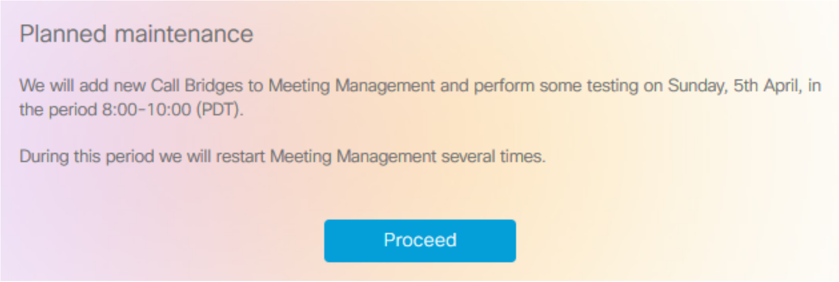
  Note: If you have lost connection to an instance of Meeting Management then you can also deregister from the Cisco SSM.

- **Disable and deregister**: You can disable Smart Licensing for Meeting Management and at the same time deregister this instance. Choose to only deregister if you want to go back to evaluation mode. Chose **Disable and deregister** if you want to stop using Smart Licensing for this Meeting Management.

16.7 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.

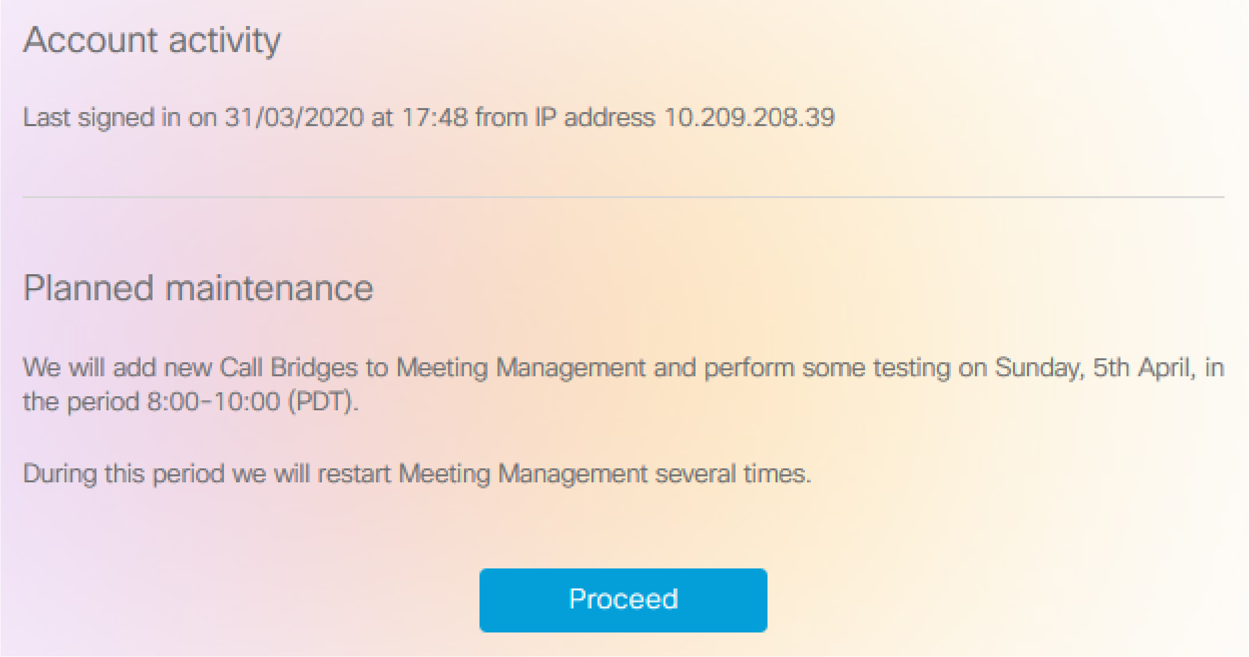


Planned maintenance

We will add new Call Bridges to Meeting Management and perform some testing on Sunday, 5th April, in the period 8:00-10:00 (PDT).

During this period we will restart Meeting Management several times.

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.



Account activity

Last signed in on 31/03/2020 at 17:48 from IP address 10.209.208.39

Planned maintenance

We will add new Call Bridges to Meeting Management and perform some testing on Sunday, 5th April, in the period 8:00-10:00 (PDT).

During this period we will restart Meeting Management several times.

Note: The changes will take place immediately.

16.8 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.

16.8.1 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 are given the message **Too many sign in attempts. Please try again later**. This happens even if the credentials are correct.

16.8.2 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.

16.8.3 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

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.

16.9 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
  - 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

16.9.1 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.

16.9.2 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
     - 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
   - **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.

16.10 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.

Document revision history

Table 1: Document revision history

Date	Description
2020-04-08	Document published.
2020-04-30	In the "Provisioning - Allow users to create spaces" section, we have updated a note with "If you use Meeting Management version 2.9.0". The issues described has been fixed in Meeting Management version 2.9.1 and later.

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.

Cisco Trademark