Contents

1 Introduction .......................................................................................................................... 4
  1.1 What is new in 2.8 ........................................................................................................ 4
    1.1.1 Changes to this guide since 2.7 ........................................................................ 4
  1.2 The software .................................................................................................................. 4

2 Deployment overview ......................................................................................................... 5
  2.1 Authentication of users ............................................................................................... 6
  2.2 Security and auditing .................................................................................................. 6
  2.3 Diagnostics and troubleshooting ................................................................................ 6
  2.4 Resilience ...................................................................................................................... 7
  2.5 Integration with Cisco TelePresence Management Suite (TMS) ......................... 7
  2.6 Connection to the Cisco Smart Software Manager for Smart Licensing ........... 8
  2.7 If you are using the Cisco Meeting Server API or 3rd party tools .................... 8

3 Overview - view notifications and license status ....................................................... 9

4 Meetings - monitor and manage meetings ................................................................. 11

5 Users - Add users or edit user settings ....................................................................... 12
  5.1 About users .................................................................................................................. 12
  5.2 Edit LDAP server details ............................................................................................ 13
  5.3 Add LDAP groups ......................................................................................................... 13
    5.3.1 Add LDAP user groups .......................................................................................... 13
  5.4 Optional: Set up security policies for local users .................................................... 14
  5.5 Set up security policies for local users ....................................................................... 14
  5.6 Add local users ............................................................................................................ 15

6 Servers - add or edit Call Bridges ................................................................................ 16

7 Logs - logs, crash reports, detailed tracing ............................................................... 19
  7.1 Log bundle .................................................................................................................... 19
  7.2 System logs .................................................................................................................. 19
  7.3 Audit logs ..................................................................................................................... 20
  7.4 Crash reports ............................................................................................................... 20
  7.5 Detailed tracing ........................................................................................................... 20
  7.6 Add or edit log servers ............................................................................................... 20
8 Licenses - view summary and events .................................................................23
  8.1 Summary .................................................................................................23
  8.2 Events ........................................................................................................28

9 Settings - configure Meeting Management ....................................................29
  9.1 Edit network details ..................................................................................29
  9.2 Upload certificate ......................................................................................29
  9.3 Edit CDR receiver address .........................................................................30
  9.4 Connect to TMS ........................................................................................30
   9.4.1 Associate cluster with TMS .................................................................31
  9.5 Get access to TMS phonebooks ................................................................32
  9.6 See NTP status or add NTP servers ..........................................................33
  9.7 Optional: Enable Smart Licensing .............................................................33
   9.7.1 Actions after you have registered .........................................................36
  9.8 Display messages when users sign in .........................................................36
  9.9 Configure advanced security settings .......................................................37
   9.9.1 Rate limit sign-in attempts ....................................................................37
   9.9.2 TLS settings .........................................................................................38
  9.10 Backup and restore ..................................................................................39
   9.10.1 Create a backup ................................................................................39
   9.10.2 Restore a backup ................................................................................39
  9.11 Restart Meeting Management ..................................................................40

10 Security hardening .......................................................................................42

Document Revision History .............................................................................43

Cisco Legal Information ..................................................................................44

Cisco Trademark .............................................................................................45
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 2.8

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

1.1.1 Changes to this guide since 2.7

We have added the following sections:

- Enable Smart Licensing
- Get access to TMS phonebooks

We have made changes to the following sections:

- Deployment overview: Added a section on connecting to the Cisco Smart Software Manager (Cisco SSM) and updated the architecture diagrams to include the Cisco SSM.
- Add Call Bridges: Added optional step for using CRL checks.
- Optional: Connect to TMS: Added optional step for using CRL checks.
- Add log servers: Added optional step for using CRL checks.

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 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

2.5 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.

### 2.6 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. 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. Meeting Management sends daily usage reports to the Cisco SSM, and the Cisco SSM then reports back whether the deployment is in compliance.

**Note:** For resilient deployments, 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 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

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.*
Overview - view notifications and license status

- **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.

- **Status not available**: License status is not supported for this cluster. You will see this information for clusters running Meeting Server version 2.5 or lower, as license status is only supported for Meeting Server version 2.6 or later.

The blue bell icon is displayed for a cluster if a new status update hasn’t 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 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 Optional: Set up security policies for local users

#### 5.5 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:

- 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.
5.6 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.

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

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 an actual cluster, the other Call Bridges in the cluster are auto–discovered and displayed as unmanaged Call Bridges below.
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 `edit`, or click anywhere in the row.
2. Edit details.
3. Click **Done**
7 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.

7.1 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.

7.2 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.
7.3 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.

7.4 Crash reports

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

7.5 Detailed tracing

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

7.6 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
8 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.

8.1 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

### License summary (90 days)

<table>
<thead>
<tr>
<th>License type</th>
<th>Installed</th>
<th>90 day peak</th>
<th>Required</th>
<th>Status</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared Multiparty Plus</td>
<td>108</td>
<td>113</td>
<td>15</td>
<td>Out of compliance</td>
<td>Acknowledge</td>
</tr>
<tr>
<td>Personal Multiparty Plus</td>
<td>50</td>
<td>45</td>
<td>0</td>
<td>Over 50% threshold</td>
<td>Acknowledge</td>
</tr>
<tr>
<td>Recording &amp; Streaming</td>
<td>158</td>
<td>80</td>
<td>0</td>
<td>In compliance</td>
<td></td>
</tr>
</tbody>
</table>

### License utilization

![Graph showing license utilization over time](image-url)
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
8.2 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.
9 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.

9.1 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.

9.2 Upload certificate

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

You must replace the self-signed certificate with a certificate signed by a CA (certificate authority).

**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.

   Note: You can restart now or wait until you have completed settings for CDR receiver address and connecting to TMS.

**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.

### 9.3 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.

### 9.4 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 the TMS 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.

### 9.4.1 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.

### 9.5 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 no contacts
- 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.

### 9.6 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.

### 9.7 Optional: Enable 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](http://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.
9.7.1 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.

- **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. Choose Disable and deregister if you want to stop using Smart Licensing for this Meeting Management.

9.8 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, 18th August, in the period 8:00- 10:00 (PDT).
During this period we will restart Meeting Management several times.

[Proceed]
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 example](image)

**Account activity**

Last signed in on 07/31/2019 at 6:02 PM from IP address 192.0.2.0

**Planned maintenance**

We will add new Call Bridges to Meeting Management and perform some testing on Sunday, 18th August, in the period 8:00-10:00 (PDT).
During this period we will restart Meeting Management several times.

![Planned maintenance message](image)

**Note:** The changes will take place immediately.

### 9.9 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.

#### 9.9.1 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.

### 9.9.2 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 suites are disabled:

- ECDHE-RSA-DES-CBC3-SHA
- DES-CBC3-SHA
- 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.

### 9.10 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

#### 9.10.1 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.

#### 9.10.2 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.
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.

9.11 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.
10 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

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
</table>
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.

© 2019 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)