Cisco Meeting Management

Cisco Meeting Management 2.9

Installation and Configuration Guide

April 16, 2021

Contents

1 Introduction

This guide is for administrators of Cisco Meeting Management, providing instructions on how to install and configure Cisco 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 video operators to monitor and manage meetings that are running on the Meeting Server.

2 What is new in 2.9

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

2.1 Changes to this guide since 2.8

We have made changes to the following sections:

- Before you start: We have updated supported Meeting Server versions.
- Optional: Configure advanced security settings: We have added a section on idle session timeout. Also, we have removed some cipher suites that are no longer available.
- Before you start: We have added a note to the Smart Licensing section about the local license file.

3 Before you start

Before you start, you need to make sure that your environment meets the requirements of Meeting Management. Also, you need to have some information ready, such as details about your network settings.

Meeting Management can manage anything from a single Call Bridge to multiple clustered deployments. The VM requirements depend on your deployment size. See the capacity table below to determine your deployment size.

3.1 Capacity

	Small to medium deployments	Large deployments
Call Bridges	1-8 Call Bridges on Cisco Meeting Server 1000 or 1 Call Bridge on Cisco Meeting Server 2000 or 1-4 Call Bridges run on X3 server	9-24 Call Bridges run on Cisco Meeting Server 1000 or 2-3 Call Bridges run on Cisco Meeting Server 2000 or 5-10 Call Bridges run on X3 server
Call legs started (at peak time, across all Call Bridges)	10 call legs started per second	20 call legs started per second
Users signed in to Meeting Management at the same time	15 concurrent users	25 concurrent users
Meetings per week (across all Call Bridges)	10,000	10,000

3.2 Requirements for the Meeting Management VM

Check that your VM environment can provide the needed specifications for your deployment size.

Requirement	Small and medium deployments	Large deployments
Server manufacturer	Any	Any
Processor type	Intel / AMD	Intel / AMD
Processor frequency	2.0 GHz	2.0 GHz
vCPU	4 cores	8 cores
Storage	100 GB *We recommend thick provisioning and eager zeroing.*	100 GB *We recommend thick provisioning and eager zeroing.*
RAM	4 GB reserved memory	8 GB reserved memory
Hypervisor	ESXi 6.0 U3, ESXi 6.5, ESXi 6.7	ESXi 6.0 U3, ESXi 6.5, ESXi 6.7
Network interfaces	1	1

Note: The VM is configured for small to medium deployments. For large deployments, you must change the sizing manually during setup.

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

3.3 Resilience

To add resilience to your Meeting Management deployment, you can connect up to 2 instances of Meeting Management to the same Meeting Server deployments.

Decide if you want to set up 1 or 2 instances of Meeting Management. They must be configured independently; each instance gets its information directly from the connected Call Bridges and from TMS. No information is exchanged between them. We recommend that the 2 instances of Meeting Management are placed in different locations so for example power outages or connection issues will not affect both instances at the same time.

Also, decide how you want to direct users to the appropriate instance of Meeting Management. The options are:

a. **Users manually sign in to a specific instance.** Define an address (FQDN) for each instance and ask users to sign in to one. If they experience issues, they should sign in to the other instance and inform their administrator.

b. **User traffic is redirected.** On top of defining an address (FQDN) for each instance, create a third, user facing address which redirects to one instance. Ask users to always sign in to the user facing address. If there are issues, the administrator should change the redirect.

Note: Even if your users are using just one user facing address at all times, each instance of Meeting Management must have a unique CDR receiver address.

Note: We recommend that you create a certificate for each instance of Meeting Management. Each certificate must include both the user facing address and the unique CDR receiver address. See Certificate for Meeting Management.

3.4 Network details, CDR receiver, and NTP

You need to know the following details before you set Meeting Management up on your network (terminal setup):

- Hostname for your Meeting Management
- IPv4 and/or IPv6 address

  You can enter manually, or choose DHCP/SLAAC
- Default gateway, if not using DHCP/SLAAC
- IP address for 1 DNS server, if required

Other details can be added when you complete the first time setup:

- CDR receiver address

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

  Note: Make sure that you set up a DNS record for your Meeting Management. Also, make sure that any firewalls are open for Call Bridges to reach the FQDN you set up for Meeting Management as CDR receiver address.
- IP or FQDN for up to 5 NTP servers, and any corresponding NTPv3 symmetric keys

  We recommend that you use the same NTP server for Meeting Management as you are using for connected Call Bridges and for your TMS server.
- Optional: IP for an additional DNS server

3.5 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: Because we recommend using LDAP in production environments, Meeting Management will always display a warning if LDAP has not been configured.

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.

3.6 User access via LDAP

For general use and administration of Meeting Management we recommend that users are authenticated via LDAP, so you should set up an LDAP server with the LDAP groups you need. We recommend that you create at least one group for administrators and one group for video operators.

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

Supported LDAP implementations are:

- Microsoft Active Directory (AD)
- OpenLDAP

  Note: memberOf overlay must be enabled for OpenLDAP

You need the following to connect to your LDAP server:

- Protocol (LDAP/LDAPS)
- LDAP server address
- LDAP server port number
- LDAP server certificate, if you are using LDAPS

  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 LDAP server address should be included in the certificate.*
- Credentials for your LDAP bind user

  For security and auditing reasons, we recommend that you create a separate bind user account for Meeting Management.
- Base distinguished name (DN)
- Search attribute

  This is the LDAP attribute you want users to enter as username when they sign in.

For adding groups, you need:

- Distinguished name for each group

3.7 Local user access

We recommend that you have at least one local administrator user to make sure you can still sign in if there are issues with your LDAP setup. You can also use local users for test purposes or for making changes to your LDAP setup.

Note: For general use in production, we recommend that all users, both administrators and video operators, are authenticated via LDAP.

During installation, Meeting Management will create a local administrator user account which you can use to sign in to the web interface and complete the setup. The username and a generated password will be displayed in the VM console when you have set up Meeting Management on your network.

Note: After you sign in to the web interface for the first time, the generated credentials are only displayed on the console until the first time you restart Meeting Management. We recommend that you change the password immediately after you sign in.

You need the following to set up more local users:

- Username for each user

  Note: A username cannot be changed after you have saved a user profile.

- Optional: First name for each user
- Optional: Last name for each user
- Role for each user
- Password for each user, if required

  If you choose to use the built-in passphrase generator, you can use the generated passwords instead of defining them yourself.

  Users can change their password after they sign in.

3.8 Security policy settings for local users

You can set up the following security policies for local users:

- 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.

3.9 Supported browsers

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

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

The following technologies must be enabled:

- WebSocket
- HTML5
- JavaScript

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

3.10 System log servers

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

We strongly recommend that you set up external system log servers. System logs are required for troubleshooting and support.

You need the following for connecting your log server to Meeting Management:

- Server address and port number
- Protocol (UDP/TCP/TLS)
- Certificate, if using TLS

Note: TLS connections must support TLS 1.2

Note: If you want to see all messages in full length, you must use a system log server that can accept and show messages with a length of up to 8192 bytes.

3.11 Audit log servers

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

Log storage has been restricted on Meeting Management, and locally stored audit logs are only available with the local system logs. However, separate audit logs can be sent to a remote location as syslog records. You can configure up to 5 external syslog servers to collect audit logs.

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

You need the following for connecting your log server to Meeting Management:

- Server address and port number
- Protocol (UDP/TCP/TLS)
- Certificate, if using TLS

Note: TLS connections must support TLS 1.2

Note: If you want to see all messages in full length, you must use a system log server that can accept and show messages with a length of up to 8192 bytes.

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

3.12 Smart Licensing

If you want to convert to Smart Licensing, you need to have a Smart Account for your company, and you need to have a Virtual Account for your Cisco Meeting Server deployment on the Cisco Software Central. Note that each Meeting Management deployment can only use one Virtual Account. If you have several clusters and want to keep licenses separate, you need to connect different clusters to different Meeting Management deployments that are each connected to a different Virtual Account.

Also, you need to determine whether you want to connect directly to the Cisco Smart Software Licensing (Cisco SSM), or if you need a proxy. If you need a proxy, you can use your own, or you can use the Cisco Transport Gateway.

For purely on-premises environments it is possible to use Cisco Smart Software Manager On-Prem which only connects at specific times to exchange data. Meeting Management supports version 7 or later.

If you want to see detailed license utilization data, you must enter the number of purchased licenses manually. You can see the exact number purchases of each license type on the Cisco Smart Software Manager.

Note: Reservation is currently not available for Cisco Meeting Server deployments.

Note: Even if Smart Licensing is enabled, a local license file is still required in Cisco Meeting Server Call Bridge. Otherwise, it will show the evaluation mode banner.

3.13 Connection to CSSM for Smart Licensing

If you want to change to Smart Licensing, then you need to connect Meeting Management to the Cisco Smart Software Licensing (Cisco SSM). If your environment does not allow direct connection, you will need to either set up a proxy server of your own, or you can download and install the Cisco Transport Gateway.

3.14 Certificate for Meeting Management

Meeting Management uses a certificate to identify itself to browsers and to Call Bridges.

During setup, Meeting Management generates a self-signed certificate which you can use during initial configuration. In a production environment, you must replace the self-signed certificate with a certificate signed by a CA (Certificate Authority). You can use an internal or external CA, depending on the requirements in your organization.

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. You can use the SAN (Subject Alternative Name) field of the certificate if more addresses are needed.

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

Note: Meeting Management has no capability to create certificate signing requests. Use a dedicated tool, for instance the OpenSSL toolkit, to create your private key and a certificate signing request.

Note: If you are setting up 2 instances of Meeting Management, we recommend that each instance has its own certificate

3.15 Call Bridge or cluster prerequisites

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

- **A user account on the Meeting Server API** . Meeting Management connects to Cisco Meeting Servers via the API. For security and auditing reasons, we recommend that you set up a separate account for Meeting Management. If you are using more than one instance, then you need a separate account for each instance of Meeting Management.

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

- **Optional: Settings required for Move participant**. If you want to move participants between meetings, there are specific requirements to your Meeting Server deployment. In particular, note that participants using SIP endpoints cannot be moved if they are provisioned through Cisco Expressway. In addition, load balancing must be configured on the Meeting Server.

  For more information, see "Limitations when moving a participant" in the *Cisco Meeting Server Administrator Quick Reference Guide: Moving a participant between conferences using the API*
- **Optional: All licenses included on all Call Bridges**. In clusters, all user licenses, as well as recording and streaming licenses, must be included in the license file for each Call Bridge. If any of these licenses are not included on all Call Bridges, then Meeting Management may report incorrect license information and compliance status. To see how licenses should be shared within a cluster, refer to the "Appendix C" of the Cisco Meeting Server *Scalability & Resilience Server Deployment Guide*.

For each Call Bridge, you need the following when you configure Meeting Management:

- IP address or FQDN for your Web Admin Interface
- Port number for the Web Admin Interface
- Username and password for the API user account that you have set up to use for Meeting Management
- If using a trusted certificate for verification, you need the CA certificate for the Web Admin Interface.

3.16 Supported Cisco Meeting Server versions

Make sure that your Meeting Server version is supported with Meeting Management.

Recommended	Minimum
2.9 or later	2.7 or later

Note: Cisco Meeting Server version 2.7 is only supported with Meeting Management until its End of Software Maintenance. For details, see the Cisco Meeting Server 2.9 release notes.

3.17 Supported TMS versions

Recommended	Minimum
15.9 or later	15.7 or later

Note: TMS versions lower than 15.9 do not support using TMS phonebooks to look up contacts in Meeting Management.

3.18 TMS prerequisites

Before installing and configuring Meeting Management, ensure your deployment meets the following requirements:

- **Call Bridges connected to TMS**. All your Meeting Server clusters must be connected to TMS.

  For instructions, see the "Cisco Meeting Server (Acano) / TMS Integration and Scheduling API Guide". You can find it under "Configuration Examples and TechNotes" on the Cisco Meeting Server Documentation page.

- **A Site Administrator user account**. For security , troubleshooting, and auditing reasons, we recommend that you set up a separate account for Meeting Management. If you are using more than one instance of Meeting Management, then create a separate account for each of them.

  For instructions, see the TMS API documentation, *Cisco TelePresence Management Suite Extension Booking API Programming Reference Guide*.

  Note: The same account is used for accessing TMS phone books and for getting information about scheduled meetings.

- **NTP server**. A time server must be configured for your TMS server to make sure that Call Bridges and your TMS server are synchronized. We recommend using the same NTP servers for your Meeting Management and for your TMS .

- **Optional: Automatic MCU failover disabled** . In case of failure, **Automatic MCU failover** moves scheduled meetings from one system in TMS to another. This could be from one Meeting Server deployment to another, but it could also be to a different type of system, such as MCU.

  As a result, a meeting may appear as scheduled in Meeting Management, but it will never become active, and video operators cannot monitor or manage the meeting using Meeting Management.

  For instructions, see the online help in TMS.

- **Optional: Same names for clusters in TMS and Meeting Management**. For administrators, it is helpful if you use the same name in TMS for the Meeting Server deployment as you use as cluster display name in Meeting Management. For operators, it is helpful if the name for the primary Call Bridge in Meeting Management can easily be associated with the name for the Meeting Server deployment in TMS.

- **Optional: Phonebook contacts using supported protocols.** if you want to use TMS phonebooks in Meeting Management, then make sure that all contacts in the phonebooks you assign to Meeting Management can be reached by your Meeting Servers.

No extra TMS license is required for you to connect Meeting Management to TMS.

CAUTION: When Meeting Management is integrated with TMS and you have many scheduled meetings, you may experience performance issues with TMS. For instance, notification emails could be delayed, or meetings would start slightly late.

The impact depends on how many meetings you schedule per week and how often you synchronize manually, as well as sizing of your TMS and its SQL database servers.

You need the following information when you connect TMS to Meeting Management:

- IP address or FQDN for the TMS booking API servers
- CA certificate for TMS, if required
- Credentials for the Site Administrator user account you have set up for Meeting Management on TMS

For each Cisco Meeting Server deployment, you need the following information from TMS:

- **TMS System ID**: The identifier TMS assigns to a connected Cisco Meeting Server deployment.

  *To find the TMS System ID: In TMS, navigate to the deployment and go to the go to its **Settings** tab, then **View Settings**, **General** area.*

- **Primary Call Bridge**: The Call Bridge in a cluster that TMS connects to.

  *To see which Call Bridge TMS is connected to: navigate to the deployment and go to the go to its **Settings** tab, then **View Settings**, **General** area. The **Network Address** is the IP address for the connected Call Bridge.*

3.19 Port information

Table 1: Ports for outgoing communication from Meeting Management

Purpose	Protocol	Destination Ports
Syslog	TCP, UDP	514 (or as configured)
Syslog	TLS	6514 (or as configured)
LDAP	LDAP	389 (or as configured)
LDAP	LDAPS	636 (or as configured)
LDAP Global Catalog (where base DN is specified to DC level only)	LDAP	3268 (or as configured)
LDAP Global Catalog (where base DN is specified to DC level only)	LDAPS	3269 (or as configured)
Time synchronization (NTP)	UDP	123
Name resolution (DNS)	UDP	53
TMS Booking API	HTTP	80
TMS Booking API	HTTPS	443
Certificate Distribution Points	HTTP	80
Smart Licensing direct	HTTPS	443
Smart Licensing via your own proxy	HTTPS	443 (or as configured)
Cisco Transport Gateway	HTTPS	443

Table 2: Ports for incoming communication to Meeting Management

Purpose	Protocol	Destination Ports
Web interface	HTTPS	443

Table 3: Ports for both incoming and outgoing communication to Meeting Management

Purpose	Protocol	Destination Ports
Cisco Meeting Server API Cisco Meeting Server CDR Meeting Server events	HTTPS	443 (or as configured on the MMP of the Meeting Server)

4 Overview of first time setup

Before you start setting up Meeting Management, please see Before you start and make sure that you have everything ready.

Meeting Management is available as an OVA file on cisco.com for all customers with a Cisco Meeting Server support contract.

During the first time setup, you will go through the following steps:

1. Deploy the OVA.
2. Set Meeting Management up on your network.
3. Sign in with generated credentials and change password.
4. Edit settings:
    a. Edit network settings.
    b. Upload certificate.
    c. Enter CDR receiver address.
    d. Optional: Connect to TMS.
    e. Optional: Get access to TMS phonebooks.
    f. Add NTP servers.
    g. Optional: Enable Smart Licensing.
    h. Optional: Add sign-in messages.
    i. Optional: Configure advanced security settings.
5. Add log servers.
6. Restart Meeting Management to save CDR receiver address, and optionally TMS details, before you add Call Bridges.
7. Add Call Bridges.
8. Optional: Associate cluster with TMS
9. Add more users:
    a. Set up LDAP server details.
    b. Add LDAP groups.
    c. Optional: Set up security policies for local users.
    d. Optional: Add local users.
10. Restart Meeting Management to save all settings.
11. Create a backup.

5 Deploy the OVA

Note: If your vCenter server release is below 6.5.0b, then **Deploy OVF Template** will not be available in the HTML5 client. If this is the case, you must use the Flash client for this step.

Note: The instructions are based on a Flash client. Your vSphere client may differ slightly from what is described below.

To deploy the OVA:

1. Sign in to your VMware environment.
2. Click **Actions**, then **Deploy OVF Template...**.
3. Select **Local file**, then browse to the OVA you have downloaded from cisco.com.
4. Continue through the wizard to select name and location, resource, storage, and network details.

   Note: If you are asked for IP Allocation settings, leave them blank. Meeting Management has its own configuration and does not use this information.

5. Make sure that the VM's memory is reserved:
   a. Go to the **Configure** tab.
   b. From the **Settings** drop-down, select **VM Hardware**.
   c. Click **Edit**.
   d. On the **Memory** tab, check **Reserve all guest memory (All locked)**.
6. If your deployment is large (see the Capacity table), change the VM Hardware settings:
   a. Go to the **Configure** tab.
   b. From the **Settings** drop-down, select **VM Hardware**.
   c. Click **Edit**.
   d. Change **CPU** from 4 to 8.
   e. Change **Memory** from 4 GB to 8 GB.
7. When your new Meeting Management VM is deployed, power it on.

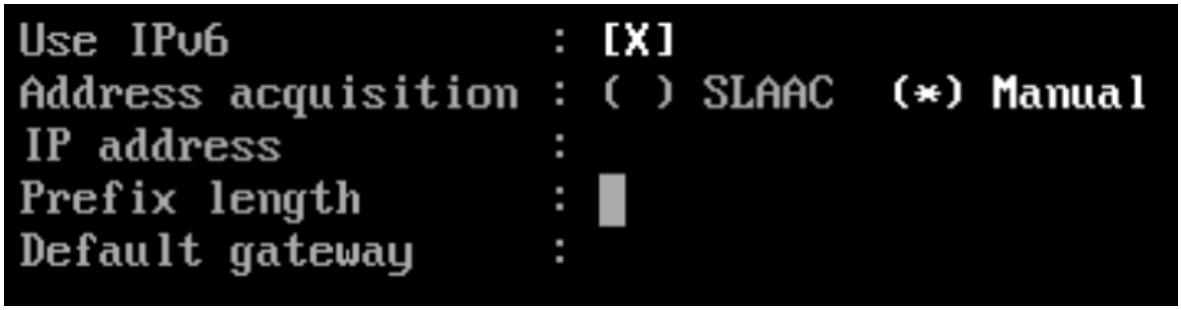
6 Set Meeting Management up on your network

Note: During the network setup via terminal, Meeting Management checks that input has the right format, but it does not perform a full verification. Please check the entered details carefully.

Note: The terminal assumes US keyboard layout. Be aware when you want to type special characters. For instance, if you have a UK keyboard, press SHIFT+2 to type @.

To set Meeting Management up on your network:

1. Open the console for the VM you just deployed.
2. To enter the setup, choose **Next**.
3. Enter a hostname for your Meeting Mangement.
4. Choose whether you want to use IPv4.
5. Choose whether you want to use **DHCP** or **Manual** address acquisition.
6. If you chose **Manual**, enter **IP address**, **Subnet mask**, and **Default gateway**.
7. Choose whether you want to use IPv6.
8. Choose whether you want to use **SLAAC** or **Manual** address acquisition.
9. If you chose to not use SLAAC, enter **IP address**, **Prefix length**, and **Default gateway**.



Note: Square brackets for IPv6 addresses are not allowed in these fields.

10. If required in your network, enter an IP address for a DNS server.

    You can only add one DNS server during this setup, but you can add one more later via the browser interface.

Note: Square brackets for IPv6 addresses are not allowed in this field.

11. Go to **Done** and press enter. Wait for your Meeting Management to start.

    The console will display one or more IP addresses, a set of generated credentials, and fingerprints for your self-signed certificate.

    Note: It may take a few minutes before your Meeting Management is ready for you to sign in to the web interface.

    Note: After you sign in to the web interface for the first time, the generated credentials are only displayed on the console until the first time you restart Meeting Management. We recommend that you change the password immediately after you sign in.

7 Sign in to the web interface and change password

Use your the generated credentials to sign in to your Meeting Management. During the sign-in process, you can change your password.

The first thing you will see is an overview page with notifications. The notifications that you see when you first sign in should disappear when you complete the configuration.

Note: The warning **There are no synchronized NTP sources** will typically not be seen, but may appear for a short while until Meeting Management has synchronized with the default NTP server.

8 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.

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

9 Upload certificate

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 your self-signed certificate.
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.*

10 Enter 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.

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

11 Optional: 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.

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.

12 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.

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

13 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, 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.

13.1 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.

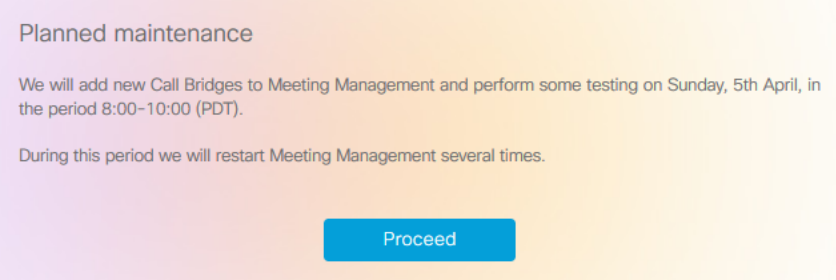
  Note: If you have lost connection to an instance of Meeting Management then you can also deregister from the Cisco SSM.

- **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.

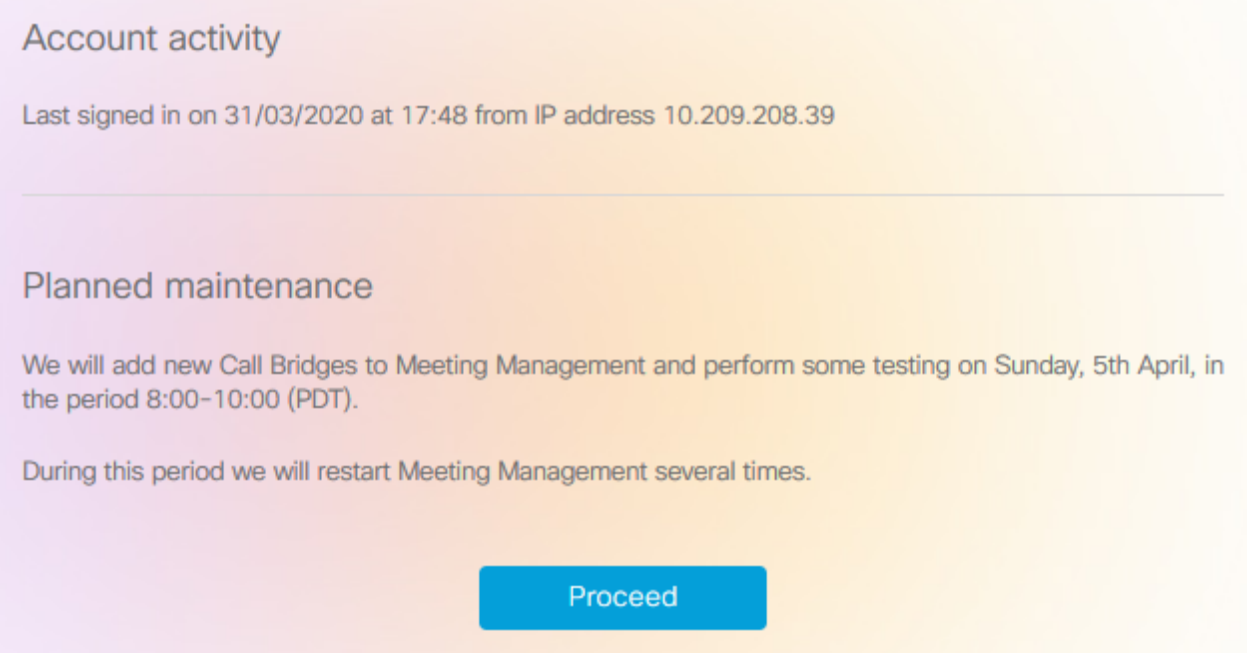
14 Optional: Add messages to display when users sign in

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

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



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



Note: The changes will take place immediately.

15 Optional: 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.

15.1 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.

15.2 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.

15.3 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 Add 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

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

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

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

   ---

17 Add Call Bridges

On the **Servers** page you can see and edit all your connected Meeting ServerCall 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 user 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**

18 Optional: 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.

19 Optional: 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.

20 Set up LDAP server

Note: All user groups must be configured on your LDAP server before you can configure Meeting Management to use them.

20.1 Set up LDAP server

To set up Meeting Management to use your LDAP server:

1. On the **Users** page, go the **LDAP** tab.
2. Check the **Use LDAP** check box.
3. Choose protocol.

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

   Default port numbers:

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

   Note: If you are using AD, and your base DN is set on domain component (DC) level only, use the default ports for searching the Global Catalog - for LDAP port 3268, for LDAPS port 3269.

   Note: If your LDAP server address is a literal IPv6 address, enter it within square brackets.

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 LDAPS, click **Upload certificate** to add the certificate chain for your LDAP server to your Meeting Management trust store.

   Certificate requirements:

   - *The certificate chain should include the certificate of the CA that signed the LDAP server'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 LDAP server must be included in the LDAP server certificate.*

7. Enter bind DN and password.

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

   Note: These fields are case sensitive.

   ---

8. Add **Base DN** (base distinguished name).

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

   Note: This field is case sensitive.

   Note: If your base DN is set on domain component (DC) level only, use the default ports for searching the Global Catalog – for LDAP port 3268, for LDAPS port 3269.

   ---

9. Choose **Search attribute**.

   The search attribute is the LDAP attribute you want users to enter as username when they sign in to Meeting Management.

   Note: This field is case sensitive.

10. **Save** your settings and **Restart** Meeting Management.

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

21 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.

21.1 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.

22 Optional: 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. You can restart now or wait until you have completed the initial configuration.

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.

23 Optional: 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.

24 Check, save, and back up

Check that all details are correct and complete, and then restart Meeting Management if required. You will notice a banner in the top of the screen if a restart is required to save your configuration.

Take a backup of your configuration, and you are ready to start using Meeting Management!

25 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

25.1 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.

You can now start using Meeting Management!

25.2 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.

26 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.

Document revision history

Table 4: Document revision history

Date	Description
2021-04-16	A note about the local license file is added to the Smart Licensing section of Before you start.
2020-04-08	Document published.

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

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)