Cisco Meeting Management

Cisco Meeting Management 3.7

Installation and Configuration Guide

June 05, 2026

Contents

Document revision history 5

1 Introduction 6

2 What is new in 3.7 7

2.1 Changes to this guide since 3.6 7

3 Before you start 8

3.1 Capacity 8

3.2 Requirements for the Meeting Management VM 9

3.3 Resilience 9

3.4 Network details, CDR receiver, and NTP 10

3.5 Users 11

3.6 User access via LDAP 12

3.7 Local user access 13

3.8 Security policy settings for local users 15

3.9 Supported browsers 15

3.10 System log servers 16

3.11 Audit log servers 16

3.12 Licensing of the Meeting Server 17

3.13 Certificate for Meeting Management 18

3.14 Call Bridge or cluster prerequisites 19

3.15 Supported Cisco Meeting Server version 20

3.16 Supported TMS versions 20

3.17 TMS prerequisites 20

3.18 Port information 23

4 Overview of first time setup 24

5 Deploy the OVA 26

6 Set Meeting Management up on your network 27

7 Sign in to the web interface and change password 29

8 Edit network details 30

9 Upload certificate 31

10 Enter CDR receiver address 32

11 Optional: Connect to TMS 33

12 Add NTP servers 35

13 Optional: Add messages to display when users sign in 36

14 Optional: Configure advanced security settings 37
14.1 Rate limit sign-in attempts 37
14.2 Idle session timeout 37
14.3 Reset meeting server password 38
14.4 TLS settings 38

15 Add log servers 40

16 Add Servers 43
16.1 Add Configured Server 43
16.2 Configure New Server 47
16.2.1 Staging 47
16.2.2 Adding a new Meeting Server 47

17 Certificate 51
17.1 CA Signed Certificate 51
17.1.1 New certificate via CSR 51
17.1.2 Use Existing Certificate and Key 53
17.2 Self Signed Certificate 54

18 Network 55
18.1 Deleting a DNS or NTP server 55

19 Call Bridge 57

20 Web Bridge 58

21 Conferencing User 59
21.1 Customizing the LDAP Search and user mappings 61

22 Security 64

23 Push Configuration 65
23.1 SSH capability 65

24 Choose licensing mode 66
24.1 How to enable Smart Licensing 66
24.2 Smart Licensing actions after Smart Licensing has been enabled 68
24.3 License Reservation 68
24.3.1 License Reservation 69
24.3.2 Update reserved licenses 72
24.3.3 Returning reserved licenses 73
24.3.4 Things to consider while migrating to Smart license 74

25 Optional: Associate cluster with TMS 76

26 Optional: Get access to TMS phonebooks 77

27 Set up LDAP server 79
27.1 Set up LDAP server 79

28 Add LDAP groups 82
28.1 Add LDAP user groups 82

29 Optional: Set up security policies for local users 83

30 Optional: Add local users 84

31 Check, save, and back up 86

32 Backup and restore 87
32.1 Create a backup 87
32.2 Restore a backup 87

32 Upload keys to validate upgrade images 90

33 Restart Meeting Management 91

Accessibility Notice 92

34 Accessibility support features 93
34.1 Keyboard navigation 93
34.2 Screen reader support 93

Cisco Legal Information 94
Cisco Trademark 95

Document revision history

Table 1: Document revision history

Date	Description
2025-06-05	Document last updated

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 manages licensing and provides a user-friendly interface to the Meeting Server.

As a Meeting Management administrator, you can:

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

A video operator can:

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

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

2 What is new in 3.7

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

2.1 Changes to this guide since 3.6

- We have updated the Hypervisor requirements for Meeting Management VM.
- We have updated the procedure to reset the Meeting Server password.
- We have updated procedure to upgrade to a special build from version 3.7

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

Table 2: Capacity table for determining the deployment size

Type	Small to medium deployments	Large deployments
Call Bridges	1-8 Call Bridges run on Cisco Meeting Server 1000 or 1 Call Bridge run on Cisco Meeting Server 2000	9-24 Call Bridges run on Cisco Meeting Server 1000 or 2-3 Call Bridges run on Cisco Meeting Server 2000
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

Note: The numbers of Call Bridges listed are primarily based on expected call volume. If all connected clusters have the meeting management functionality disabled, then the VM requirements for small deployments will be sufficient for any deployment size.

3.2 Requirements for the Meeting Management VM

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

Table 3: Requirement for Meeting ManagementVM

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 6.5 P09, 6.7 P08, 7.0 U3j	
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.

Note: If you disable meeting management for all clusters then you do not need a CDR receiver address, but Meeting Management will show an error notification.

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

Note: 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. Administrators can tag video operators to specific spaces, giving them access to the meetings associated with those spaces only.

- **Video operators** only have access to the **Meetings** and **Overview** pages. Video operators monitor and manage meetings, and they perform basic troubleshooting related to ongoing meetings. For instance, they may try to call a participant who got disconnected or check the call statistics if someone has audio issues. Video operators will have permission to perform the tasks related to meetings held in the space as assigned by the administrator.

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

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

3.6 User access via LDAP

For general use and administration of Meeting Management, we recommend that users are authenticated via LDAP. You should set up an LDAP server with the necessary LDAP groups. We recommend creating at least one group for administrators and another for video operators. If authentication issues occur, LDAP users can reset their passwords on the LDAP server and then log in to Meeting Management again.

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.

In case of authentication issues, local users can reset their credentials with the assistance of other administrators by using the **Unlock** button available in the **Local** tab on the **Users** page. This allows an administrator to provide new credentials for the locked-out user. If the local administrator encounters authentication issues and they are the only administrator account available, the password cannot be recovered. In such cases, the local administrator user must re-install Meeting Management after removing all the existing data.

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
- Microsoft Edge
- 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 Licensing of the Meeting Server

Meeting Management is mandatory with Meeting Server 3.0 or later as Meeting Server depends on Meeting Management for licensing.

For each instance of Meeting Management, you can choose Smart Licensing or no licensing.

For resilient deployments, use only one instance of Meeting Management for licensing to avoid double reporting of usage. Set the licensing mode to Smart Licensing on one instance, and set it to no licensing for the other instance.

Note: All Meeting Server clusters must be connected to an instance of Meeting Management that has licensing enabled. Only disable licensing for one instance of Meeting Management if you have a resilient deployment and the other instance of Meeting Management has licensing enabled.

For Smart Licensing you need the following:

- You must have a Smart Account for your company with a dedicated Virtual Account that will be used by only one instance of Meeting Management.

  To request an account, talk to your Cisco account team or go to Cisco Software Central.

- The appropriate licenses must be allocated to the Virtual Account that Meeting Management will use.

  Note that one Virtual Account can be connected to one instance of Meeting Management. Also note that all licenses in one Virtual Account are shared between all the clusters that are connected via Meeting Management.

  If you wish to license a cluster separately, then connect it to a different Meeting Management deployment and Virtual Account.

- You need to determine whether you can connect directly to the Cisco Smart Software Manager, or if you need a proxy. You can use your own proxy server, or you can use the Cisco Transport Gateway.

  *If are using a proxy server, then you must have address and port number available so you can **Edit Transport Settings**.*

- Optional: For purely on-premises environments it is possible to use Cisco Smart Software Manager On-Prem (SSM On-Prem) which only connects at specific times to exchange data. Meeting Management supports version 8-202008 or later.

  Note: If you try to connect to Cisco Smart Software Manager On-Prem and it refuses to authorize Meeting Management, log into your SSM On-Prem and check whether the authorization is failing due to the **Active Call Bridge Node** license. If yes, resynchronize SSM On-Prem to your Smart Account and the problem will be fixed.

  *If 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 gateway address, use the format http://<SSM onprem address>/SmartTransport **or** https://<SSM onprem address>/SmartTransport depending on your setup.*

3.13 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

3.14 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.** To get information about meeting activity, 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.

  Note: If you use Meeting Management only for licensing and provisioning for a cluster, then you do not need CDR capacity on Call Bridges in that cluster.

- **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*

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.

Note: The VM must be shut down using the MMP command 'shutdown'. This ensures that the Meeting Server sends an appropriate disconnect message to all connected devices including participants in a meeting and Meeting Management.

If the Meeting Server VM is abruptly turned off/shutdown during an active meeting, although the participants will be disconnected, they will still appear to be connected, and the Audio/Video Mute buttons will remain in a loading state until the connection to the Meeting Server is restored.

3.15 Supported Cisco Meeting Server version

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

Meeting Management 3.7.0 is only supported with Cisco Meeting Server version 3.7.0.

3.16 Supported TMS versions

Table 4: Recommended version

Recommended	Minimum
15.10 or later	15.9 or later

3.17 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.*

3.18 Port information

Table 5: 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
Webex Cloud and Control Hub	HTTPS	443 (or as configured)

Table 6: Ports for incoming communication to Meeting Management

Purpose	Protocol	Destination Ports
Web interface	HTTPS	443

Table 7: 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. Add NTP servers.
    f. Optional: Add sign-in messages.
    g. 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.
    a. Add an existing Meeting Server
    b. Configure and add a new Meeting Server
8. Choose licensing mode
9. Optional: Associate cluster with TMS
10. Optional: Get access to TMS phonebooks.
11. 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.

12. Restart Meeting Management to save all settings.
13. 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.
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.

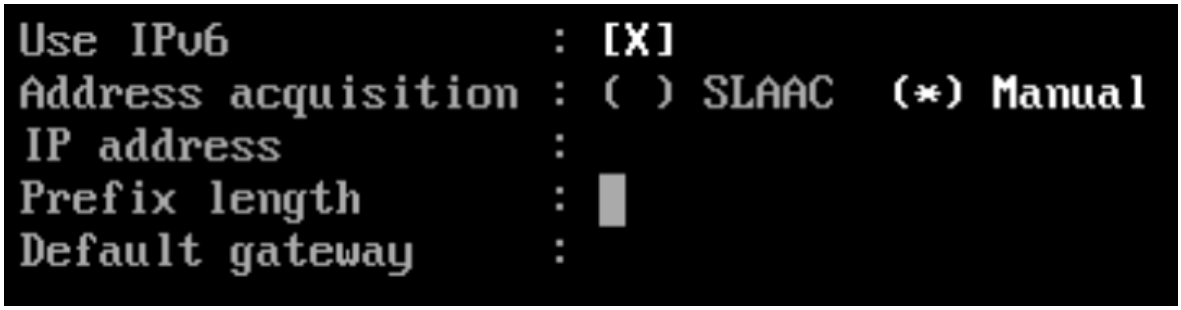
6 Set Meeting Management up on your network

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 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.
3. Note: If you type in IPv6 addresses, do not use square brackets here.
4. 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.*

  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.

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.*

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

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

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

12 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.

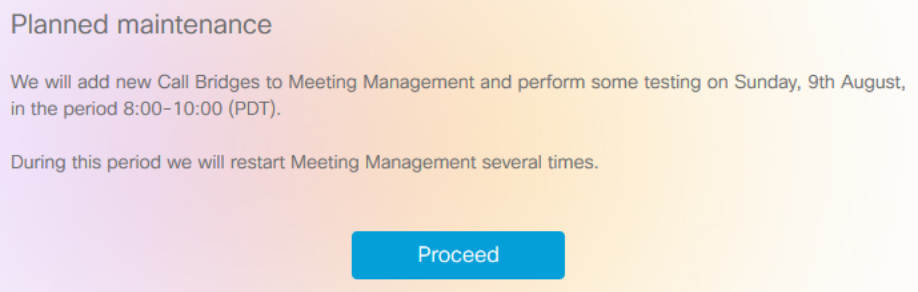
3. To save the changes, Restart your Meeting Management.

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

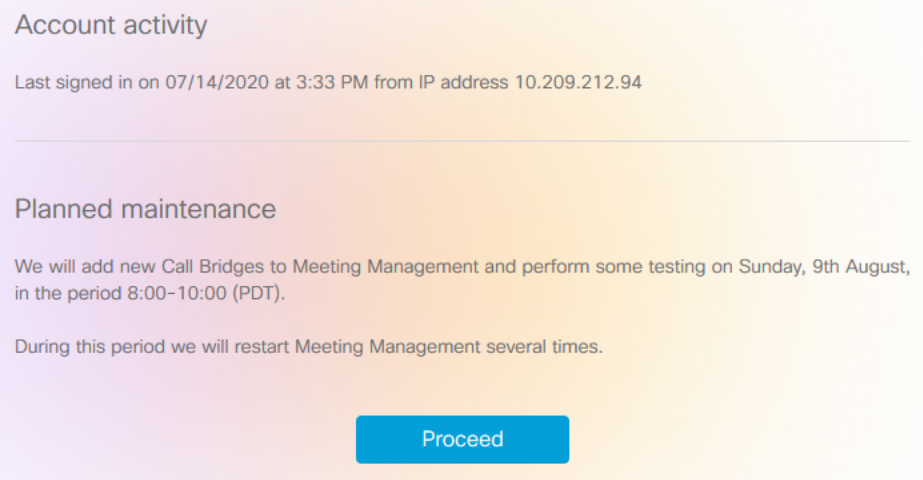
13 Optional: Add messages to display when users sign in

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.

14 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.

14.1 Rate limit sign-in attempts

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

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

There are two settings:

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

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

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

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

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

14.2 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.

14.3 Reset meeting server password

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

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

The following setting is displayed:

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

14.4 TLS settings

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

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

- Browsers
- LDAP server
- Call Bridges
- System log servers
- Audit log servers
- TMS
- Cisco Smart Software Manager

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

By default, the following cipher suite is disabled:

- AES256-SHA

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

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

15 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.

   ---

16 Add Servers

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

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

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

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

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

To add a Call Bridge or Edge Node:

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

16.1 Add Configured Server

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

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

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

   This is the same as your Web Admin Interface address.

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

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

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

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

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

4. Enter a **Display name**.

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

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

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

   We recommend that you enable this when possible.

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

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

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

   Certificate requirements:

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

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

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

   Note: You can change this later by editing cluster settings, see instructions in the *User Guide for Administrators*.

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

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

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

To add auto-discovered Call Bridges and Edge Nodes:

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

To edit a Call Bridge or Edge Node:

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

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

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

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

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

16.2 Configure New Server

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

16.2.1 Staging

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

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

New Meeting Server Instances

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

Existing Meeting Server Instances

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

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

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

16.2.2 Adding a new Meeting Server

To complete server configuration tasks you will also need:

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

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

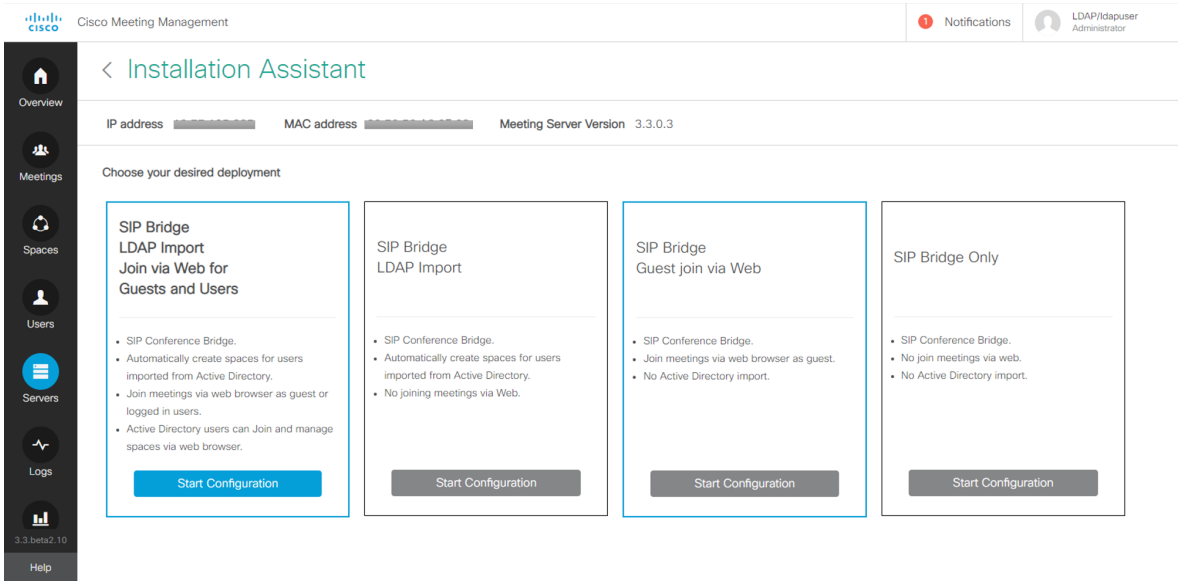
1. In the **Installation Assistant** page, enter **Server address** of the Meeting Server.
2. Enter the **Username** configured on the Meeting Server.

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

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

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

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



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

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

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

17 Certificate

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

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

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

17.1 CA Signed Certificate

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

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

17.1.1 New certificate via CSR

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

Completing this process requires:

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

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

Steps for creating a new certificate request (CSR):

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

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

   Table 8: Fields required for a Certificate Signing Request

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

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

Error Scenarios

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

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

17.1.2 Use Existing Certificate and Key

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

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

Steps for using an existing certificate:

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

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

Error Scenarios

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

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

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

17.2 Self Signed Certificate

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

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

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

Steps for using a self-signed certificate:

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

Error Scenarios

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

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

18 Network

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

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

1. Configure the following:

Table 9: Description of the fields to be filled ffor configuring network settings

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

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

18.1 Deleting a DNS or NTP server

1. Click to delete the DNS/ NTP server.

Error Scenarios

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

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

19 Call Bridge

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

1. Enter the following details:

Table 10: Description of the fields to be filled for setting Call Bridgeservice

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

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

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

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

Error Scenario

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

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

20 Web Bridge

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

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

Error Scenario

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

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

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

21 Conferencing User

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

Creating user accounts requires:

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

If you wish to create user accounts:

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

   Details on each setting are provided in the following table:

Table 11: Configuring the LDAP connection

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

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

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

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

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

Error Scenarios

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

21.1 Customizing the LDAP Search and user mappings

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

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

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

Table 12: LDAP Import settings

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

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

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

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

Error Scenarios:

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

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

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

22 Security

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

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

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

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

Error Scenarios:

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

- If the entered username is incorrect.
  Solution: You must provide a valid username.
  Note: Enter an alphanumeric value other than 'admin'.
- If the entered password and confirmation passwords do not match.
  Solution: Re-enter the same passwords in both the fields.
  Note: You must provide only alphanumeric values.

23 Push Configuration

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

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

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

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

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

23.1 SSH capability

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

24 Choose licensing mode

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

You must choose a licensing mode. Choose between:

- **Smart Licensing** (recommended)

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

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

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

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

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

Note:

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

24.1 How to enable Smart Licensing

To enable Smart Licensing:

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

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

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

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

    Note:

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

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

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

24.2 Smart Licensing actions after Smart Licensing has been enabled

You can do the following:

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

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

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

24.3 License Reservation

To be compliant with SMART, Cisco product users require support for License Reservation. Meeting Management supports license reservation from version 3.4 onwards. In an environment where Meeting Management cannot connect to the Internet due to security reasons, License reservation can be used to activate features and reserve licenses.

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

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

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

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

License reservation allows the following workflows:

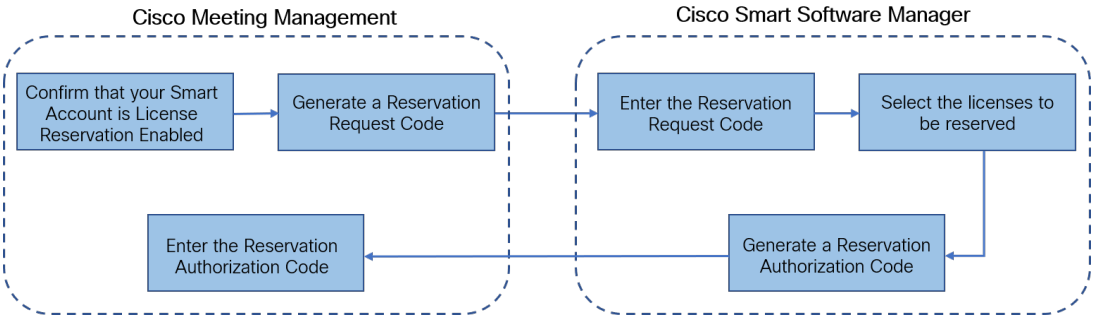
- Reserve SLR/PLR licenses
- Update reserved licenses
- Return reserved licenses

24.3.1 License Reservation

The workflow for initial license reservation is as follows:

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

Figure 1: Workflow for License Reservation



Follow these steps for license reservation:

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

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

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

    ---

    c. Enter the Reservation Request Code.
    d. Choose licensing from **Licenses to Reserve**:
        - For PLR - Select option **Meeting Server PLR Enablement**
        - For SLR - Select option **Reserve a specific license** and select the specific licenses to be reserved.
    e. Click **Generate Authorization Code** button to generate the Reservation Authorization Code.
    f. Save or copy the Reservation Authorization Code.

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

    ---

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

5. The license status in the **Licenses** page will be displayed as:
    - **Reservation Active** for PLR
    - **Reserved** along with the number of licenses for SLR.

24.3.2 Update reserved licenses

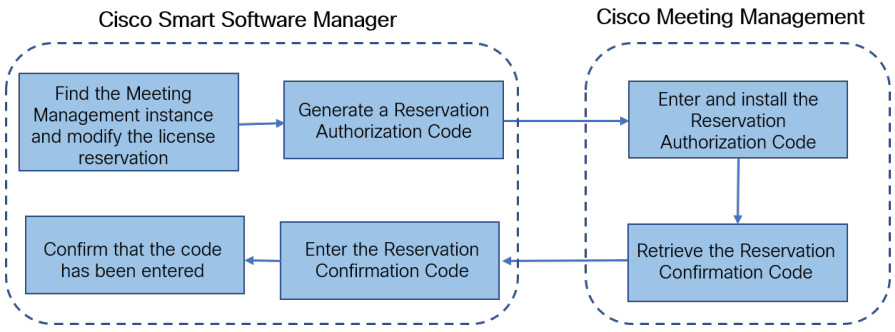
To meet the changing needs of your organization, you can update specific licenses or you can change the number of reserved licenses. For example, your current license requirement is 5 and you want to add another 5 licenses, then you need to select the number of licenses as 10 and the new value overrides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

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

The workflow for updating reserved license is as follows:

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

Figure 2: Workflow for Update License Reservation



Follow these steps to update the reserved licenses:

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

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

    ---

    c. Click **Install Authorization Code** button to update license reservation and to generate a Reservation Confirmation Code.
    d. Copy or save the Reservation Confirmation Code by clicking **View confirmation code** button in **Smart Software Licensing** page.
3. In Cisco Smart Software Manager,
    a. Find Cisco Meeting Management instance in **Product Instances** and select **Enter Confirmation Code...** from the **Actions** menu to launch the **Enter Confirmation Code** pop-up.
    b. Enter the Reservation Confirmation Code into the **Enter Confirmation Code** pop-up.
    c. Return to the **Smart Software Licensing** page in Meeting Management and click **Code Has Been Entered** button to dismiss the alert that was placed after the Reservation Authorization Code was installed.

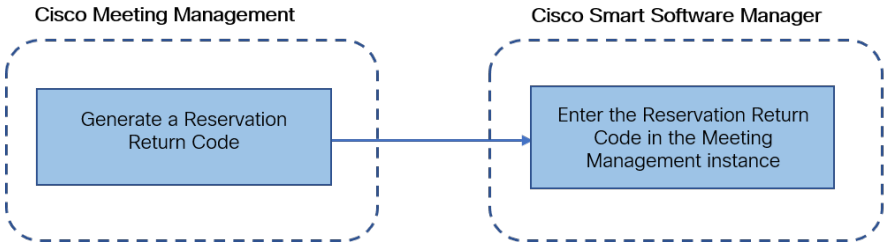
24.3.3 Returning reserved licenses

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

The workflow for returning a reserved license is as follows:

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

Figure 3: Workflow for Returning License Reservation



Follow these steps to return reserved license:

1. In the **Licensing** section of Meeting Management **Settings**,
   a. Click **Return Reserved Licenses...** button to launch the **Confirm Return Licenses** pop-up.
   b. Click **Generate** button to generate a Reservation Return Code.
   c. The **License Reservation Return Code** pop-up provides instructional text and allows to copy or download a file containing the License Reservation Return Code.
2. In Smart Software Manager,
   a. Find the Meeting Management instance in **Product Instances**
   b. Select **Remove** from the **Actions** menu to launch the **Remove Product Instance** pop-up.
   c. Enter the Reservation Return Code into the pop-up to complete returning reserved licenses. The **Registration** status is changes to **Deregistered** in the **Licensing** page.

24.3.4 Things to consider while migrating to Smart license

1. Existing traditional licensing files (PAK files) can be used for upgrading to 3.4 version.

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

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

   ---

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

25 Optional: Associate cluster with TMS

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

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

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

26 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.

27 Set up LDAP server

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

27.1 Set up LDAP server

To set up Meeting Management to use your LDAP server:

1. On the **Users** page, go the **LDAP server** 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.

28 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.

28.1 Add LDAP user groups

To add a user group:

1. On the **Users** page, go to the **LDAP user groups** tab.
2. Click **Add LDAP group**.
3. Enter **LDAP path**.
4. Click **Check** to see if the group is found.
5. If the group is found, click **View users** to check if you see the usernames you expected to see in this group.
6. Select a role for the group.
7. Click **View User Profile** button available in **Actions** against the selected user to launch **User Profile** pop-up window.
8. Click **Next**.
9. 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.
10. Click **Done**.
11. Restart Meeting Management

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

29 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:

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

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

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

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

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

  Dictionary requirements:

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

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

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

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

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

  1. Restart Meeting Management

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

30 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.

To edit a local user:

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

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

To unlock a user:

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

31 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!

32 Backup and restore

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

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

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

32.1 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.

32.2 Restore a backup

Before you restore a backup:

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

  The password was chosen when you or another administrator created the backup.
- Decide if you want to restore all settings, or if you just want to restore either database or configuration details (see step 4 below).

- Make sure that your LDAP server is online while you restore the backup.
- If you have TMS connected, make sure TMS is online while you restore the backup.

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

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

To restore a previously saved backup:

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

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

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

Note:

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

32 Upload keys to validate upgrade images

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

Image signatures are only verified when upgrading from a signed image. So manual verification is still advised when upgrading from an unsigned image to a signed image. i.e. if you upgrade from 3.6 to 3.7, or downgrade to earlier versions, you are still advised to manually verify the hashes. This feature will be fully effective when upgrading from 3.7 and beyond.

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

To upload public keys:

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

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

33 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.

Accessibility Notice

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

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

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

You can find more information about accessibility here:

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

34 Accessibility support features

34.1 Keyboard navigation

You can use your keyboard to navigate through Meeting Management.

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

34.2 Screen reader support

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

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

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

Cisco Legal Information

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

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

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

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

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

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

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

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

© 2023 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)