



# Cisco TelePresence Management Suite Provisioning Extension with Cisco Unified CM

## Deployment Guide

**Last Updated: August 2020**

Cisco TMSPE 1.14

Cisco TMS 15.8/15.9/15.10/15.11/15.12

Cisco Unified CM 12.5

TelePresence Conductor XC 4.3





# Contents

<b>Introduction</b>	<b>7</b>
This Deployment Guide	7
Related Documents	7
<b>Prerequisites and Recommendations</b>	<b>8</b>
Estimating Your Deployment Size	8
Hardware Requirements	9
Regular Deployment and Cisco Business Edition 6000	9
Large Deployment	9
Recommended Hardware and Virtualization for Large Deployments	10
Cisco TMSPE server software and configuration requirements	11
SMTP server requirements	11
SQL Server software and permission requirements	12
Cisco Collaboration Meeting Rooms Hybrid Requirements	12
Cisco TelePresence Conductor	12
Cisco Unified Communications Manager	12
	13
Required security permissions	13
For installation	13
For operation	13
TLS Support	13
Information needed during installation	13
Cisco TMS username and password	13
Database information	14
Database location	14
Feature options during installing	14
User import requirements	14
Service account	15
Secure connection	15
Active Directory	15

LDAP .....	15
Browser requirements .....	15
Administrator interface .....	15
User portal .....	15
Licensing requirements .....	15
Best practices for deployment .....	16
Automate user creation and management with AD/LDAP .....	16
Use secure communication .....	16
Multiparty Licensing .....	16
<b>Installing Cisco TMSPE .....</b>	<b>18</b>
Installing Cisco TMSPE with a Redundant Cisco TMS Setup .....	18
Upgrading from Previous Versions to Cisco TMSPE 1.14 .....	18
High-level Workflow .....	18
Upgrading Cisco TMSPE .....	18
Performing a New Installation .....	19
Enabling Cisco TMSPE .....	19
<b>Setting up Users .....</b>	<b>22</b>
Creating Groups and Adding Users .....	22
Setting up Groups .....	22
Importing users from external directories .....	22
Adding Users Manually .....	26
Configuring and Sending Account Information .....	26
Configuring Email Settings .....	26
Sending Account Information to a Single User .....	28
Sending Account Information to All Users in a Group .....	28
<b>Deploying Smart Scheduler .....</b>	<b>29</b>
Best Practices and Limitations .....	30
Booking Limitations .....	30
User Access to Smart Scheduler .....	31
Access Rights and Permissions .....	32
Time Zone Display .....	32
WebEx Booking .....	32
How Smart Scheduler Works .....	33
<b>Deploying Collaboration Meeting Rooms .....</b>	<b>33</b>
What are Collaboration Meeting Rooms? .....	33
Room Size and Quality .....	33

PIN Protection .....	33
How Collaboration Meeting Rooms Are Created .....	33
Differences from TelePresence Conductor-created Conferences .....	34
Collaboration Meeting Room Resource Consumption .....	34
Setting up Collaboration Meeting Room .....	34
Before You Start .....	34
Connecting to TelePresence Conductor .....	35
Creating Templates .....	35
Applying Templates to Groups .....	40
Setting up Host and Guest Roles in CMRs .....	40
Host Privileges .....	40
Allowing the Guest Role .....	41
Disallowing the Guest Role .....	41
Including WebEx Participants in CMR meetings .....	41
Before you start .....	41
Enabling WebEx in CMRs .....	42
Making Changes that Affect Collaboration Meeting Rooms .....	42
Modifying or Replacing the Template for a Group .....	42
Deleting Templates .....	43
Deleting Users .....	43
Moving Users Between Groups .....	43
Touch Tones and DTMF .....	43
Auto-connected Participants .....	44
Add a Favorite Auto-connected Participant .....	44
Modify a Favorite Auto-connected Participant .....	44
<b>Maintaining Users .....</b>	<b>45</b>
Synchronizing User Data .....	45
Mapping of LDAP and AD Fields .....	45
Testing a Manual Synchronization .....	45
Running a Manual Synchronization .....	46
Moving Users and Groups .....	46
Moving User Accounts Imported from External Sources .....	46
Searching for User Accounts .....	46
Renaming Groups and User Accounts .....	46
Updating Cisco TMS Connection Details .....	47
<b>Maintaining the Databases .....</b>	<b>48</b>

Backing up the Databases .....	48
Moving or Renaming the Databases .....	48
<b>Troubleshooting .....</b>	<b>49</b>
Running Cisco TMSPE Diagnostics .....	49
Running a health check .....	49
Viewing system status .....	49
Restarting the TMS Provisioning Extension Windows Service .....	50
Logs .....	50
Cisco TMSPE and Cisco TMS Logs .....	50
Troubleshooting the Installation .....	50
Checking the Installation Log .....	50
Unable to Establish SQL Connection Through Java Runtime... ..	51
Unable to Find Valid Certification Path to Requested Target .....	51
Portal Troubleshooting .....	51
Cannot Access FindMe or Smart Scheduler .....	51
<b>Uninstalling Cisco TMSPE .....</b>	<b>51</b>
Using the Installer .....	51
Using the Control Panel .....	52
Reusing or Replacing the Existing SQL Database When Reinstalling .....	52
<b>Appendix 1: ady Using Personal Multiparty Licensing with Cisco TMSPE .....</b>	<b>52</b>
Limitations .....	52
Combining Licenses .....	52
Feature Support .....	53
Applying License Restrictions to CMR Templates .....	53
Tracking the Number of Licenses Used .....	54
<b>Notices .....</b>	<b>54</b>
Accessibility Notice .....	54
Obtaining Documentation and Submitting a Service Request .....	54
<b>Cisco Legal Information .....</b>	<b>55</b>
<b>Cisco Trademark .....</b>	<b>55</b>

## Introduction

Cisco TMS Provisioning Extension (Cisco TMSPE) is an application for Cisco TMS that offers the following features for telepresence users and administrators:

- Smart Scheduler, a web-based telepresence scheduling tool for end users.
- Collaboration Meeting Rooms, permanent personal telepresence virtual spaces that also support WebEx.

Cisco TMSPE provides both administrator configuration and end-user interfaces for these features. End users can access Collaboration Meeting Room and Smart Scheduler in a common portal.

For deployments with Cisco TelePresence Video Communication Server (Cisco VCS), Cisco TMSPE also includes large-scale user provisioning and FindMe, a user-configurable telepresence call forwarding feature. For guidance, see *Cisco TMSPE with Cisco VCS Deployment Guide*.

## This Deployment Guide

This guide covers the deployment and maintenance of Cisco TMSPE 1.14 with Cisco TMS version 15.7 and Unified CM.

The document provides:

- requirements, best practices and step-by-step instructions for installing Cisco TMSPE to the Cisco TMS server
- instructions for deploying each of the available Cisco TMSPE features
- typical maintenance tasks for Cisco TMSPE administrators, and a troubleshooting section

## Related Documents

All documentation for the latest version of Cisco TMSPE can be found at [http://www.cisco.com/en/US/products/ps11472/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps11472/tsd_products_support_series_home.html).

Title	Link
<i>Cisco TMSPE Release Notes</i>	<a href="http://cisco.com">http://cisco.com</a>
<i>Cisco TMS Installation and Getting Started Guide</i>	<a href="http://cisco.com">http://cisco.com</a>
<i>Cisco TMS Administrator Guide</i>	<a href="http://cisco.com">http://cisco.com</a>
<i>How to enable Windows Installer logging</i>	<a href="http://support.microsoft.com/kb/223300">http://support.microsoft.com/kb/223300</a>
<i>Distinguished Names</i>	<a href="http://msdn.microsoft.com">http://msdn.microsoft.com</a>
<i>Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters (RFC4515)</i>	<a href="http://tools.ietf.org/html/rfc4515">http://tools.ietf.org/html/rfc4515</a>

### Training

Training is available online and at our training locations. For more information on all the training we provide and where our training offices are located, visit [www.cisco.com/go/telepresencetraining](http://www.cisco.com/go/telepresencetraining)

### Glossary

A glossary of TelePresence terms is available at: [tp-tools-web01.cisco.com/start/glossary/](http://tp-tools-web01.cisco.com/start/glossary/)

## Prerequisites and Recommendations

This section describes prerequisites and best practices for installing and deploying Cisco TMSPE.

### Estimating Your Deployment Size

The requirements for Cisco TMS depend on and grow with the size and complexity of the deployment. The complexity of an installation is driven primarily by the volume of activity and number of endpoints controlled by and bookable in Cisco TMS.

Use the following chart to identify the relative size of your deployment. If your intended deployment matches multiple level criteria, apply the highest level.

	Regular and Cisco BE6000	Large
Cisco TMS	<ul style="list-style-type: none"> <li>■ &lt; 200 controlled systems</li> <li>■ &lt; 100 concurrent participants</li> <li>■ &lt; 50 concurrent ongoing scheduled conferences</li> </ul>	<ul style="list-style-type: none"> <li>■ &lt; 5000 systems that use system licenses, that is, controlled systems, systems registered to Unified CM that are added to Cisco TMS, and Unmanaged Rooms. Adding more than 5000 such systems is not supported.</li> <li>■ &lt; 1800 concurrent participants</li> <li>■ &lt; 250 concurrent ongoing scheduled conferences</li> </ul>
Cisco TMSXE	< 50 endpoints bookable in Microsoft Exchange	< 1800 endpoints bookable in on-premises Microsoft Exchange or < 1000 endpoints bookable in Office 365 or a combination of on-premises Exchange and Office 365 Note that with Office 365, latency towards Exchange is likely to be greater than for an on-premises deployment. This may lead to Cisco TMSXE occasionally saving a booking before all related events have been processed. Users will then receive multiple email notifications for the same booking.
Cisco TMSPE	<ul style="list-style-type: none"> <li>■ &lt; 1000 Collaboration Meeting Rooms</li> <li>■ &lt; 2000 Cisco VCS-provisioned users (Note: Cisco VCS provisioning not supported on BE6000)</li> </ul>	<ul style="list-style-type: none"> <li>■ &lt; 48,000 Collaboration Meeting Rooms</li> <li>■ &lt; 100,000 Cisco VCS-provisioned users</li> </ul>
Co-residency	All three applications and Microsoft SQL Server may be co-resident.	<ul style="list-style-type: none"> <li>■ Cisco TMSXE must be on a dedicated server.</li> <li>■ Cisco TMS and Cisco TMSPE must use an external SQL Server.</li> </ul>

Other factors that influence Cisco TMS performance and scale include:



- The number of users accessing the Cisco TMS web interface.
- Concurrency of scheduled or monitored conferences.
- The use of ad hoc conference monitoring.
- Simultaneous usage of Cisco TMSBA by multiple extensions or custom clients. Booking throughput is shared by all scheduling interfaces including the Cisco TMS **New Conference** page.

Actual booking speed will vary based on the meeting size, features, and schedule complexity around the meeting.

## Hardware Requirements

Find the appropriate hardware requirements below based on your estimated deployment size.

All applications including SQL Server may also be installed on virtual machines with specifications corresponding to these hardware requirements

### Regular Deployment and Cisco Business Edition 6000

In a regular deployment, Cisco TMS and extensions can be co-located on the same server.

	Requirement	Cisco BE6000
CPU	2 cores (Xeon 2.4 GHz or larger), dedicated	1 vCPU
Memory	8 GB, dedicated	4 GB vRAM, dedicated
Disk space provided on server	60 GB	60 GB

Note that Cisco TMSPE on Cisco Business Edition 6000 does not include Cisco VCS-based user provisioning for endpoints or FindMe.

### Large Deployment

In a large deployment, Cisco TMSXE and SQL Server must be external, while Cisco TMS and Cisco TMSPE are always co-resident.

#### Cisco TMS and Cisco TMSPE Server

	Requirement
CPU	2 cores (Xeon 2.4 GHz or larger), dedicated
Memory	8 GB, dedicated
Disk space provided on server	80 GB  Note: For successful running of Cisco TMS / Cisco TMSPE, 20% of disk space must be free.

#### Microsoft SQL Server

This server must be in the same time zone as the Cisco TMS server.

	Requirement
CPU	4 cores (Xeon 2.4 GHz or larger), dedicated
Memory	16 GB, dedicated
Disk space provided on server	60 GB

When planning for a large deployment, also keep in mind that:

- The disk space needed for a large **tmsng** database is typically 20-30 GB.
- The size of the three Cisco TMSPE databases will not exceed 6 GB in most deployments.
- The prime performance limiters in SQL Server are RAM and disk I/O. For optimum performance, increase these values as much as possible.

## Cisco TMSXE Server

The requirements for this server correspond to the recommended hardware requirements for the supported operating systems.

## Recommended Cisco TMS Configuration Changes

To decrease the load on SQL Server and Cisco TMS services in a large deployment, we strongly recommend the following settings :

- **Administrative Tools > Configuration > Conference Settings:** Set **Default Reservation Type for Scheduled Calls** to *One Button To Push*
- **Administrative Tools > Configuration > General Settings:** Set **Route Phone Book Entries** to *No*
- **Administrative Tools > Configuration > Network Settings:** Set **Enable Ad Hoc Conference Discovery** to *Only for MCUs* or *No*.

## Recommended Hardware and Virtualization for Large Deployments

Cisco has tested and recommends the following specifications for large deployments up to the supported maximum. Using the specifications described below, the entire Cisco TMS deployment can be hosted on a single rack-mounted server.

### Hardware

Server	Cisco UCS C220 M3S Rack Server
CPU	2 x Intel Xeon Processor E5-2430 v2 (2.50 GHz)
Disk	8 x 146GB 6G SAS 15K RPM SFF HDD/hot plug/drive sled mounted, in a RAID-6 configuration. Part number: A03-D146GC2.
Disk controller	LSI MegaRAID 9265-8i 6Gb/s
Memory	4 x 8 GB/1600 MHz
Hypervisor software	VMware ESXi 6.5 and 6.0 host the three virtual machines with the specifications described below.  Note: Cisco TMSPE has been qualified with VMware File system 5, as VMware File system 6 has a known issue with ESXi 6.5. You have to continue with File System 5, until the issue is fixed.

## Cisco TMS and Cisco TMSPE Virtual Machine

CPU	4 x vCPU
Memory	8 GB
Disk	200 GB

### Microsoft SQL Server Virtual Machine

CPU	4 x vCPU
Memory	16 GB
Disk	250 GB

### Cisco TMSXE Virtual Machine

CPU	4 x vCPU
Memory	8 GB
Disk	100 GB

## Cisco TMSPE server software and configuration requirements

Cisco TMSPE must be installed on the same server as Cisco TMS.

Product	Version and description
Cisco TMS	<ul style="list-style-type: none"> <li>■ Cisco TMS 15.8/15.9/15.10/15.11/15.12.</li> </ul>
SQL Server connection	<ul style="list-style-type: none"> <li>■ TCP/IP or Named Pipes protocol must be enabled. TCP/IP is the preferred protocol, see below.</li> <li>■ SQL Server Browser must be running and able to listen to UDP port 1434.</li> </ul>
Windows Server	<ul style="list-style-type: none"> <li>■ Windows Updates must be enabled. Note that the default connection protocol is TCP/IP. If this protocol is used, no hotfixes are required.</li> </ul>
Java	<p>Cisco TMSPE has been tested with Java 8 and its updates, 32-bit and 64-bit versions.</p> <p>Download the installer from <a href="http://www.java.com">www.java.com</a>.</p> <p><b>Caution:</b> Do not upgrade Java while Cisco TMSPE is running. Disable the Windows service prior to any upgrade. We strongly recommend disabling automatic Java updates on the server. If switching from 32 bit to 64 bit version of Java, it will require re-installation of Cisco TMSPE.</p>

### No support for multiple network cards

Multiple network cards on the Cisco TMS server are not supported. Cisco TMSPE is not supported on a server with multiple IP addresses and will only bind to the first available network interface. Multiple network cards or IP aliases on the same card are therefore not supported. Multiple IPv4 addresses and multiple IPv6 addresses are not supported, but single IPv4 address and single IPv6 addresses are supported. Cisco TMSPE cannot use multiple network cards on a server and will only bind to the first available network interface.

## SMTP server requirements

Cisco TMSPE requires a valid SMTP server that will accept SMTP relay from the Cisco TMS server to send account information to users from Cisco TMSPE.

If your SMTP server requires authentication, make sure this information is available during configuration.

## SQL Server software and permission requirements

A complete installation of Cisco TMSPE creates three databases:

- **tmspe**
- **tmspe\_vmr**
- **tms\_userportal**

For installation and upgrading, SQL Server and Windows Authentication mode (mixed mode) must be enabled on the database server. After installation is completed, mixed mode can be disabled and Windows Authentication enabled until the subsequent upgrade.

## User and database creation

When installing or upgrading Cisco TMSPE and using an existing SQL Server, the installer prompts for an SQL user and password. The default is to enter the server sa (system administrator) username and password. If the sa account is not available, use one of the following:

- Automatic setup, but with security limited role. Ask your SQL server administrator to create an SQL user and login that has the dbcreator and securityadmin server roles. This account will be the service account for Cisco TMSPE. When prompted for SQL Server credentials during installation, enter the username and password for that account. Cisco TMSPE will create the tmspe/tmspe\_vmr/tms\_userportal databases automatically using the server defaults, assign itself as the owner and continue to use the supplied account to access the databases after installation.
- Manual database creation, max security limited role. Ask your SQL server administrator to create:
  - Empty databases named **tmspe**, **tmspe\_vmr**, and **tms\_userportal** in the same instance as **tmsng** , with database collation Latin1\_General\_CI\_AS (case insensitive and accent sensitive).  
The settings **ALLOW\_SNAPSHOT\_ISOLATION** and **READ\_COMMITTED\_SNAPSHOT** must be *On*.
  - An SQL user and login to use for the Cisco TMSPE Service account and grant the user the *dbowner* role for the different databases. This permission must be kept after installation for Cisco TMSPE to function.

## Cisco Collaboration Meeting Rooms Hybrid Requirements

In order to use Cisco TMSPE for meetings that include WebEx, Cisco TMS must be set up with:

- one or more WebEx sites
- WebEx credentials for each user (not service user), either manually added or using WebEx/Cisco TMS single sign-on

For guidance on setting up Cisco Collaboration Meeting Rooms Hybrid with or without single sign-on, see [Cisco Collaboration Meeting Rooms Hybrid Configuration Guide](#).

## Cisco TelePresence Conductor

Cisco TelePresence Conductor XC 4.3 is required.

## Cisco Unified Communications Manager

Unified CM 12.5 is required.

### Routing requirements

A route pattern/dial plan must be set up on the Unified CM and on the Cisco TelePresence Conductor.

For more information on dial planning for the Unified CM, see [Cisco Unified Communications Manager Dial Plan Deployment Guide](#) and [Cisco Unified Communications Manager Administration Guide](#) .

For more information on dial planning for the Cisco TelePresence Conductor, see [Cisco TelePresence Conductor with Cisco Unified Communications Manager Deployment Guide](#).

## Required security permissions

### For installation

The following security permissions are required for installing Cisco TMSPE:

Application	User Privilege
Microsoft Windows server hosting Cisco TMS	Local Server Administrator
MS SQL	<ul style="list-style-type: none"><li>■ <i>sysadmin</i> if the installer will create the database on the MS SQL server</li><li>■ <i>db_owner</i> if using a manually created database on the MS SQL server. See <a href="#">Required security permissions, page 13</a> for further details.</li></ul>

### For operation

The following security permissions are required for operation of Cisco TMSPE:

Application	User Privilege
SQL Instance housing Cisco TMSPE Databases	<i>db_owner</i>
Cisco TMS	Member of the Site Administrator group in Cisco TMS. We recommend creating a service account for this purpose either locally or in Active Directory. For redundant deployments, use an AD account.

## TLS Support

Cisco TMSPE will communicate using SSL for connections. SSL includes HTTPS , using TLS 1.0. Cisco TMSPE does not support TLS 1.1 and TLS 1.2.

## Information needed during installation

### Cisco TMS username and password

The Cisco TMSPE installer asks for the username and password of a service user that belongs to the Site Administrator group in Cisco TMS.

These credentials will be:

- added to the corresponding fields in the **Cisco TMS Connection** settings, which can be viewed and modified after installation by going to **Administrative Tools > Configuration > Provisioning Extension Settings**.
- used by Cisco TMSPE to request data from Cisco TMS.
- used to book on behalf of Smart Scheduler users in Cisco TMS. Every time a meeting is booked or updated, an email notification will be sent to this user as well as to the meeting owner. If you do not want this email sent to the service user, the user must be set up without an available email address.

## Database information

The installer detects where the Cisco TMS SQL database (`tmsng`) is located and recommends installing Cisco TMSPE's SQL databases (`tmspe`, `tms_userportal` and `tmspe_vmr`) to the same location and instance. `tmspe`, `tms_userportal` and `tmspe_vmr` must be co-located.

In this case, the administrator needs to know the following about the `tmsng` database:

- SQL server name
- SQL server instance
- SQL server credentials with adequate privileges

## Database location

During installation, the installer offers the possibility of storing the `tmspe`, `tms_userportal` and `tmspe_vmr` databases to another location and instance. However, we recommend storing them in the same location as the `tmsng` database. Note that the database names must be `tmspe`, `tms_userportal` and `tmspe_vmr`, using the same casing and underscore.

If desired, the installer also offers the ability to use separate SQL credentials for `tmspe` to operate in. Select **Use separate SQL Credentials for the TMS Provisioning Extension** during the installation to change these credentials. See the section [Required security permissions, page 13](#) for appropriate operation permissions.

## Feature options during installing

During the installation, Cisco TMSPE will display an option to select features to install.

### Core Component

The option **Core Components** is mandatory when installing. Core Components contain the `tmspe` database and is required for provisioning.'

### User Portal

**User Portal** is optional when installing. User Portal contains the `tms_userportal` database which will be installed if User Portal is selected during installation.

User Portal contains a group of features:

- User Portal,
- FindMe and
- Smart Scheduler.

### CMR

**CMR** is also optional when installing and contains only the feature CMR. CMR contains the `tmspe_vmr` database. To install CMR you must also select and install the User Portal.

## Features and databases in Cisco TMSPE

The different features are connected to the different databases used in Cisco TMSPE. By not installing the optional features, the creation of their dependent databases can be omitted..

## User import requirements

Cisco TMSPE does not support user names that contain characters that needs to be "escaped" in an URL string.

Cisco TMSPE supports the import of users from the following external sources:

- Active Directory
- Active Directory with Kerberos

- Lightweight Directory Access Protocol (LDAP)

## Service account

You must define a service account in Active Directory that has read access to the Global Catalog. This service account must have a password with no retention policies applied to it so that the password does not expire.

## Secure connection

To achieve a secure connection, you must use either:

- Active Directory with Kerberos
- LDAP with StartTLS

Otherwise, by default the LDAP connection uses the SIMPLE bind type, which is not secure. Also, using LDAP with the SSL connection type does not provide a secure connection, as by default, all certificates will be trusted.

## Active Directory

Cisco TMSPE 1.14 has been tested with:

- Active Directory 2012
- Active Directory 2008

## LDAP

LDAP implementations other than Active Directory must have the following for import and synchronization to be supported:

- An `entryUUID` field as defined by [RFC 4530](#).
- Simple paging as defined by [RFC 2696](#).

## Browser requirements

### Administrator interface

The client requirements for the administrator interface are identical to the requirements for Cisco TMS, see [Cisco TelePresence Management Suite Installation and Upgrade Guide](#) for your version.

### User portal

The User Portal has been tested with the following browsers and versions:

- Microsoft Internet Explorer 11
- Firefox 59
- Google Chrome 65
- Safari 11.1 and above for Mac OS X and iPad

Other browsers may work, but are not actively tested and supported.

## Licensing requirements

No license is required to install Cisco TMSPE, but a license is required for some features:

Feature	License requirement
User synchronization with Active Directory	None
Collaboration Meeting Rooms	<p>No license required in Cisco TMS.</p> <p>One or more of the following required:</p> <ul style="list-style-type: none"> <li>■ Screen licenses on TelePresence Server.</li> <li>■ Appropriate MCU port licenses.</li> <li>■ Personal Multiparty Basic or Personal Multiparty Advanced. For configuration requirements specific to these licenses, see <a href="#">Appendix 1: Using Personal Multiparty Licensing with Cisco TMSPE, page 52</a>.</li> <li>■ Shared Multiparty License / Personal Multiparty License on Conductor.</li> </ul>
Smart Scheduler	None
Option key:	<ul style="list-style-type: none"> <li>■ Cisco TMS <ul style="list-style-type: none"> <li>– Cisco TMS Provisioning Extension option key</li> </ul> </li> </ul>

## Best practices for deployment

### Automate user creation and management with AD/LDAP

We recommend synchronizing users from Microsoft Active Directory or LDAP with Cisco TMSPE to automate the creation and management of users.

For Active Directory import to work:

- Active Directory and Cisco TMS must be members of the same domain.
- A service account for Cisco TMSPE in Active Directory with read access to the Global Directory must be available.

### Use secure communication

Cisco TMSPE requires a secure connection to Cisco TMS via HTTPS. When you upgrade or install Cisco TMS, the installer enables HTTPS communication. We strongly recommend using valid certificates.

### Multiparty Licensing

Multiparty Licensing lets you administer licenses centrally on the Cisco TelePresence Conductor instead of loading screen licenses locally onto the Cisco TelePresence Servers. Compared to traditional screen licensing, Multiparty Licensing allows for greater capacity at lower cost. Two variants are available:

- Personal Multiparty (PMP) licenses. Each license is assigned to a specific user. PMP licenses are suitable for users who initiate conferences frequently.  
PMP licenses are purchased through Cisco Unified Workspace Licensing (CUWL Pro). They are available for deployments with Unified CM for call control.
- Shared Multiparty (SMP) licenses. Each license is shared by multiple users, but only in one conference at a time. SMP licenses are suitable for users who initiate conferences infrequently.  
SMP licenses are available for deployments with either Unified CM or Cisco VCS for call control.  
Non Active Directory/Local users support only Shared Multiparty Licenses.



Each TelePresence Conductor can support either Multiparty Licensing or TelePresence Server screen licensing, but not both together. If you have a mix of TelePresence Server and Cisco TelePresence MCU Series conference bridges however, you can use Multiparty Licensing for the TelePresence Servers and port licensing for the MCUs together on the same Conductor.

## Installing Cisco TMSPE

This section covers the process of installing or upgrading Cisco TMSPE.

### Installing Cisco TMSPE with a Redundant Cisco TMS Setup

When installing Cisco TMSPE to a redundant Cisco TMS deployment using a network load balancer, the extension must be installed on all servers. The general installation instructions apply, with some exceptions.

The overall process is as follows:

1. Install Cisco TMSPE on one Cisco TMS server following the instructions for clean installation. See [Performing a New Installation, page 19](#).
2. Install Cisco TMSPE on the remaining servers following the same instructions for clean installation. When prompted, opt to reuse the existing database found by the installer.
3. Enable the provisioning mode only after completing the above steps. See [Enabling Cisco TMSPE, page 19](#).

For further guidance on redundancy, see the chapter "Redundant deployments" in *Cisco TelePresence Management Suite Installation and Upgrade Guide*.

## Upgrading from Previous Versions to Cisco TMSPE 1.14

### High-level Workflow

Cisco TelePresence Management Suite Provisioning Extension relies on and integrates with multiple other products.

When upgrading your deployment:

1. Upgrade Cisco TMS to the required version following the instructions in *Cisco TMS Installation and Upgrade Guide*.
2. Upgrade Cisco TMSPE.
3. Upgrade other systems such as TelePresence Conductor as required.

### Upgrading Cisco TMSPE

#### If the Server is Running Java 6 or 7

If upgrading Cisco TMSPE from 1.0 or 1.1:

Upgrading from these previous versions will require replacing Java as these Cisco TMSPE versions would be using Java 6 or 7.

1. Ensure that all critical Windows Updates are installed on your server.
2. Close all open applications and disable virus scanning software.
3. Uninstall Cisco TMSPE from the server. Do not remove any other files.
4. Uninstall the currently installed version of Java.
5. Install Java 8.
6. Extract the Cisco TMSPE installer from the zip archive to the Cisco TMSPE server.
7. Run the installer as administrator.
8. Follow the installer instructions.
9. Re-enable virus scanning software.

## Performing a New Installation

To install:

1. Ensure that all critical Windows Updates are installed on your server.
2. Close all open applications and disable virus scanning software.
3. Extract the Cisco TMSPE installer from the zip archive to the Cisco TMS server.
4. Run the Cisco TMSPE installer as administrator.
5. Follow the setup instructions:
  - a. Click **Next** to initiate the setup.
  - b. Accept the terms in the license agreement and click **Next**.
  - c. Click the icons in the tree to change the ways features will be installed.
  - d. Enter the **Username** and **Password** of the service user that Cisco TMSPE will use to connect to Cisco TMS. This user must be a member of the Site Administrators group in Cisco TMS. Click **Next**.
  - e. The installer detects where the TMS SQL database (**tmsng**) is installed. We recommend installing the Cisco TMSPE SQL databases to the same SQL instance.
    1. Confirm or enter the appropriate **SQL Server Name** and **Instance Name**, if required. If deploying in a redundant setup, make sure both installations are pointing to the same database location.
    2. Fill in the necessary credentials.
    3. Click **Next**.
  - f. Click **Install** to begin the installation. Click **Back** to review or change installation settings.
  - g. When the installation is complete, click **Finish** to exit the **Setup** window.
6. Re-enable virus scanning software.

## Enabling Cisco TMSPE

After completing the installation:

1. In Cisco TMS, go to **Administrative Tools > Configurations > General Settings**, set the field **Provisioning Mode** to *Provisioning Extension* and click **Save**. You may need to refresh the browser window or empty the browser cache after making this selection.

The screenshot shows the 'General Settings' page in Cisco TMS. The breadcrumb trail at the top right indicates 'You are here: Administrative Tools > Config'. The 'General Settings' section is active. The 'Provisioning Mode' is set to 'Provisioning Extension' (highlighted in blue). Other settings include 'TMS Release Key' (masked with dots), 'Default ISDN Zone' (ip isdn), 'Default IP Zone' (ip isdn), 'Default User Language' (English (US)), 'Software FTP Directory' (C:\Program Files (x86)\TANDBERG\TMS\www\vtms\public\data\SystemSoftware\), 'System Contact Name' (Video Help Desk), 'System Contact E-mail Address' (video@example.com), 'Global Phone Book Sort' (System Specific Sort), 'Route Phone Book Entries' (Yes), 'Cisco System Phone Books' (Use centralized TMS phone books only (corporate phone book)), 'Phone Books Update Frequency' (Every Day), 'Phone Books Update Time of Day' (5:00 PM), 'Alternate System Name Rules for Endpoints and Rooms (order of name to use)' (Use System Name only (displays "no-name" if blank)), 'Enable Auditing' (No), 'Enable Login Banner' (Off), 'Show Systems in Navigator Tree' (Yes), and 'Enable TMS Redundancy' (No). An 'Edit Login Banner' button is visible on the right.

2. Go to **Administrative Tools > Activity Status** to verify that the switch is completed.

3. Verify that Cisco TMSPE features are now available and functioning.
  - a. Browse to the following pages in Cisco TMS:
    - **Systems > Provisioning > Users**. If this page reports a problem connecting to User Repository, the database connection is not working. See [Troubleshooting the Installation, page 50](#).
    - **Systems > Provisioning > Devices**
    - **Systems > Provisioning > FindMe**  
Note that **Systems > Provisioning > FindMe** will be displayed with an error message if when/if FindMe has been enabled.
    - **Administrative Tools > Configuration > Provisioning Extension Settings**
  - b. Go to **Administrative Tools > Provisioning Extension Diagnostics**, look for any alarms raised and click **Run Health Check**. If any alarms are raised, click them to see details and perform the corrective actions described. See [Troubleshooting the Installation, page 50](#) for further information.



## Setting up Users

This section describes the required procedures to configure Cisco TMSPE for provisioning.

### Creating Groups and Adding Users

Users can be added to Cisco TMSPE by importing from an external directory, or manually adding individual users. Before users can be added, you must set up a group hierarchy.

Do not import or add users directly into the root group, as this complicates bulk deletion of users.

### Setting up Groups

Whenever you add users manually or import users from external sources into a particular group, the users inherit all settings that are assigned to the group. Any settings not assigned at the group level are inherited from the parent group.

To add a group:

1. In Cisco TMS, go to **Systems > Provisioning > Users**.
2. In the **Users and Groups** container, click the parent of the group you want to add.
3. Above the explorer view, click **Add Group**.  
The **Add Group** dialog box is displayed.
4. In the **Display Name** field, enter a name for the group.
5. Click **Save**.

You can now import users into the group from an external directory, or add users manually.

### Importing users from external directories


#### Before You Start






1. Ensure that the intended directory source is supported, see [User import requirements, page 14](#).
2. As imports are set up per group, ensure that you have added at least one group into which you want to import users, as users should not be added directly to the root group.
3. In the case of creating multiple groups that will be configured for external directory source imports, ensure that the configuration for each group import setting results in a user being found and imported into only a single group.

#### Setting up an Import

To import user accounts from an external directory:





1. In Cisco TMS, go to **Systems > Provisioning > Users**.
2. In the **Users and Groups** container, navigate to and click the group into which you want to import user accounts. Information about the selected group is displayed in a number of panes.



 **example\_group**

 Rename Group...  Delete  Send Account Information  Move Group  Toggle Details

---


**User Settings**


Name	Pattern	Origin
Video Address Pattern	{first_name}.,{last_name}@example.com	 example_group
Caller ID Pattern	{mobile_phone}	 example_group
Device Address Pattern	{username}.,{device.model}@example.com	 example_group
Image URL Pattern		 root

 Edit  Reload

---

**User Import**

 No user import has been configured for this group.

 Configure

3. In the **User Import** pane, click **Configure**.
4. If you want to copy user import settings from the parent group as a starting point, click **Copy from parent**.
5. In the **Type** field, select the type of external directory from which you are importing user data. Configuration fields will be displayed based on the type of external directory you choose to import from. The screenshot below shows the fields available for Secure AD:

**User Import**

Type: Active Directory with Kerberos (Secure AD) ▼

Hostname:

Port:

Username:

Password:

Base dn:




Relative search dn:

Search filter:

Distribution center:

Distribution center timeout:

Realm:

 Copy from parent  Save  Cancel

6. In the fields provided, specify the information that Cisco TMSPE requires to contact the external directory. Configure the fields according to the following table:

Field	Active Directory (AD)	Active Directory with Kerberos (Secure AD)	Lightweight Directory Access Protocol (LDAP)	Description
<b>Hostname</b>	Yes	Yes	Yes	Server hosting the external directory. Provide a fully qualified domain name (FQDN).
<b>Port</b>	Yes	Yes	Yes	Port on the server used for accessing the external directory. Use Global Catalog port 3268 for Kerberos import.
<b>Username</b>	Yes	Yes	Yes	User name Cisco TMSPE uses when logging on to the external directory. See also Password.
<b>Password</b>	Yes	Yes	Yes	Password Cisco TMSPE uses when logging on to the external directory. See also Username.
<b>Base dn</b>	Yes	Yes	Yes	LDAP distinguished name. See the MSDN Library article <a href="#">Distinguished Names</a> for more information.
<b>Relative search dn</b>	Yes	Yes	Yes	LDAP relative distinguished name from the Base DN (see also Base dn). The relative DN is the baseDN's relative filename to its parent folder. For example, if the DN is <code>c:\example\folder\myfile.txt</code> , the relative DN is <code>myfile.txt</code> . Detailed information on RDN can be found in the MSDN Library article <a href="#">Distinguished Names</a> .
<b>Search filter</b>	Yes	Yes	Yes	Search filter that specifies which accounts to import. Detailed information on these filters and how to construct them can be found in RFC4515: <a href="#">Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters</a> .
<b>Distribution center</b>	No	Yes	No	The address of the Kerberos Key Distribution Center server, which is the address of your Active Directory (AD). The value can either be a fully qualified domain name (FQDN) or the domain where your AD server resides, in which case a DNS SRV lookup is performed to determine the FQDN.
<b>Distribution center timeout</b>	No	Yes	No	Maximum number of milliseconds to wait for a reply from the Key Distribution Center.
<b>Realm</b>	No	Yes	No	Realm configured in AD for Kerberos Authentication.
<b>Connection type</b>	No	No	Yes	Select the connection type. The available options are: <ul style="list-style-type: none"> <li><i>Unsecured</i></li> <li><i>StartTLS</i></li> <li><i>SSL</i>— note that no certificate handling is supported for this connection type.</li> </ul>



Field	Active Directory (AD)	Active Directory with Kerberos (Secure AD)	Lightweight Directory Access Protocol (LDAP)	Description
Ignore certification errors	No	No	Yes	Select Yes or No.

7. Click **Save**.

For detail on mapping of Active Directory and LDAP fields to Cisco TMSPE attributes and instructions on performing manual synchronization, see [Synchronizing User Data, page 45](#).

### Customizing Field Mappings for Import of New Users from Active Directory/LDAP Directory

To allow integrating with customized Active Directories/LDAP Directories, Cisco TMSPE allows users to change the field mappings for users between Active Directory/LDAP and Cisco TMSPE.

Changing field mappings will only apply to new user imports, and not the ones already created. Changing field mappings will also require a restart of the Cisco TelePresence Management Suite Provisioning Extension windows service.

Any customization for the field mapping of "**External Identifier**" must comply with RFC 4530 and RFC 2696.

#### To change Active Directory/ LDAP field mapping for new user imports:

1. Go to **Administrative Tools > Configuration > Provisioning Extension Settings > Active Directory Field Mapping for New User Imports**.
2. Change the values according to your Active Directory installation.
3. Go to **Administrative Tools > Configuration > Provisioning Extension Settings > LDAP Field Mappings for New User Imports**.
4. Change the values according to your LDAP installation.
5. Click **Save**.
6. Restart the TMS Provisioning Extension windows service.

### Checking Active Directory Connection Settings

To check the connection settings and make sure the filter template is appropriate for what you want to import:

1. Go to **Administrative Tools > Configuration > Provisioning Extension Settings**.
2. Scroll to the **Active Directory Connection** settings.

#### Active Directory Connection

Connection Timeout *	<input type="text" value="5000"/>	(milliseconds)
Filter Template *	<input type="text" value="(&amp;(objectCategory=person)(sAMAccountType=80530"/>	
Follow Referrals *	<input checked="" type="radio"/> Yes <input type="radio"/> No	
<div>  Save          Cancel          Restore Default       </div>		

3. Modify the settings as desired:
  - **Connection Timeout** in milliseconds
  - **Filter Template** will be applied to all group imports. The %s variable in the template will be replaced by any **Search Filter** set for a group import.
4. Click **Save**.

## Adding Users Manually

The alternative to importing user accounts from external directories is to add user accounts manually.

Before you add user accounts, ensure that the group to which you want the accounts to belong is already in the group hierarchy. See [Adding Users Manually, page 26](#).

Also note that any manually added user will not be able to sign in to the FindMe user portal unless their manually created username matches one of the following:

- Their Active Directory username if one exists.
- A local Windows username on the Cisco TMS/Cisco TMSPE server if the user does not have an Active Directory account. If creating such an account, make sure to supply the user with the necessary credentials to sign in to the portal.

To add a user account manually:

1. In Cisco TMS, go to **Systems > Provisioning > Users**.
2. Use the search field below the heading of the **Users and Groups** container to confirm that the user account does not already exist.
3. In the **Users and Groups** container, navigate to and click the group in which you want the account to belong.
4. In the **Users and Groups** container, click **Add user**.  
The **Add User** dialog box opens.
5. Specify information about the user in the fields provided. The username must not exceed 20 characters.
6. Click **Save**.

## Configuring and Sending Account Information

To simplify the distribution of account information to users, Cisco TMSPE provides an email function with a configurable email template that can be used to inform individual users or groups of their provisioning account settings and account details for functions such as FindMe.

## Configuring Email Settings

To configure email settings:

1. In Cisco TMS, go to **Administrative Tools > Configuration > Provisioning Extension Settings**.

### Account Information Email

Sender Address \*

Subject \*

Body \* 

```
{display_name}:
Below is your provisioning account information:




Username: {username}
Password: {password}
```

SMTP Hostname \*

SMTP Port \*

SMTP Username

SMTP Password

 Save  Cancel  Restore Default

2. In the **Account Information Email** pane, configure the fields as follows:

<b>Sender Address</b>	Email address Cisco TMSPE uses as the sender email address when sending email notifications. The address appears in the <b>From</b> field of the recipient's email client
<b>Subject</b>	Subject of the email notifications. The subject appears in the <b>Subject</b> line of the recipient's email client.
<b>Body</b>	<p>Template that determines the body of the email sent to users. For an example, see the screenshot above.</p> <p>If using FindMe, we recommend adding the following additional information:  You can be contacted via your FindMe ID:  {video_address}.</p>
<b>SMTP Hostname</b>	IP-address or hostname of your SMTP (mail) server.
<b>SMTP Port</b>	Port number used by your SMTP (mail) server.
<b>SMTP Username</b>	Username to access the mail server if this is required
<b>SMTP Password</b>	Password to access the mail server if this is required.

3. Under **User Repository**, select whether to **Enable automatic email sending to imported users**. By default, this is set to *No*.

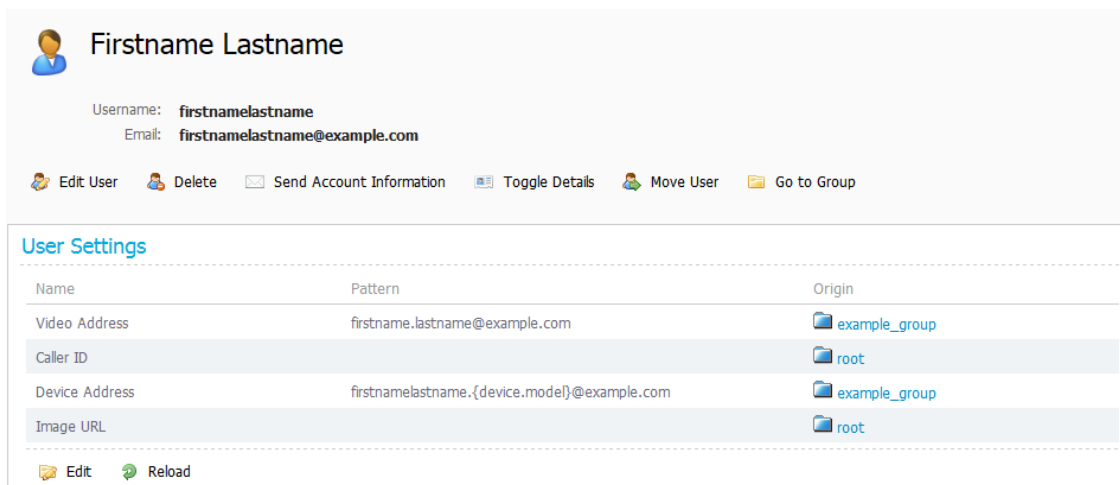
#### 4. Click **Save**.

If you import users from Active Directory and choose to enable automatic email sending, you do not need to follow the procedures below.

## Sending Account Information to a Single User

We recommend sending account information to a single user as a test, for example your own account, prior to sending account information to a large group of users:

1. In Cisco TMS, go to **Systems > Provisioning > Users**.
2. In the **Users and Groups** container, navigate to and click your own username or the username of another suitable recipient of a test email. Information about the selected user is displayed in a number of panes.



The screenshot shows the user profile for 'Firstname Lastname'. It includes fields for Username (firstname.lastname) and Email (firstname.lastname@example.com). Below these are action buttons: Edit User, Delete, Send Account Information, Toggle Details, Move User, and Go to Group. The 'User Settings' pane is expanded, showing a table of settings:

Name	Pattern	Origin
Video Address	firstname.lastname@example.com	example_group
Caller ID		root
Device Address	firstname.lastname.{device.model}@example.com	example_group
Image URL		root

At the bottom of the User Settings pane are 'Edit' and 'Reload' buttons.

3. In the area above the **User Settings** pane, click **Send Account Information**.

A message is displayed confirming that the email has been scheduled for sending.

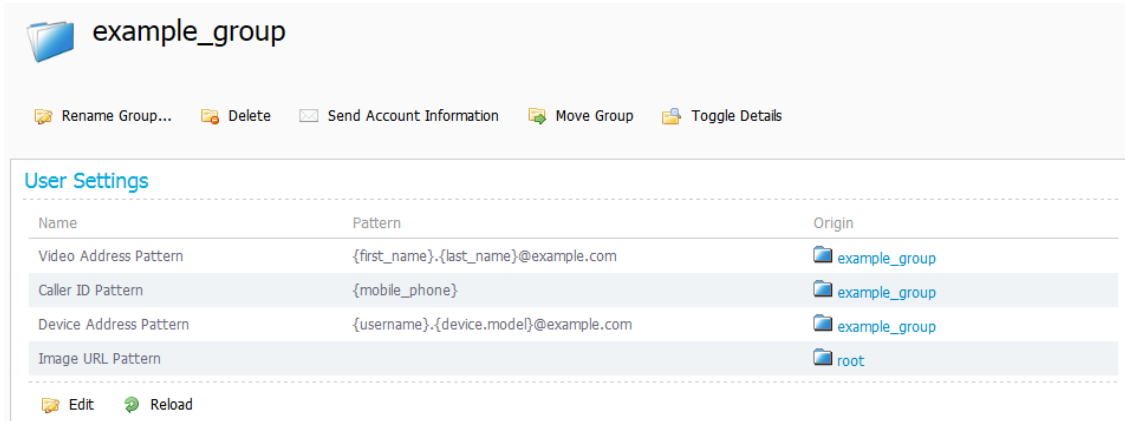
Depending on the configuration of your email server, the scheduled email should arrive in the selected recipient's inbox within a few minutes. If the email fails to be delivered, check the **Alarms** pane on the **Diagnostics** page. See [Running Cisco TMSPE Diagnostics, page 49](#).

## Sending Account Information to All Users in a Group

When you select a group to notify, Cisco TMSPE notifies all users in that group as well as users in all subgroups.

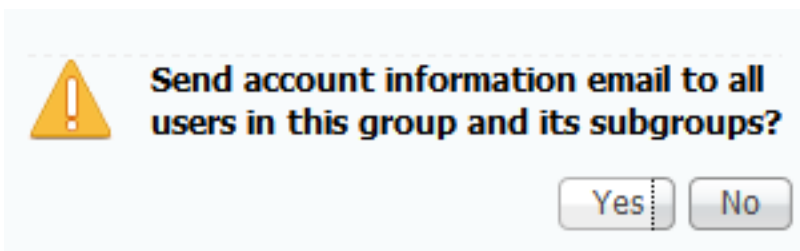
To send out account information to a group:

1. In Cisco TMS, go to **Systems > Provisioning > Users**.
2. In the **Users and Groups** container, navigate to and click the required group. Information about the selected group is displayed in a number of panes.



Name	Pattern	Origin
Video Address Pattern	{first_name}-{last_name}@example.com	example_group
Caller ID Pattern	{mobile_phone}	example_group
Device Address Pattern	{username}-{device.model}@example.com	example_group
Image URL Pattern		root

3. In the area above the **User Settings** pane, click **Send Account Information**. A confirmation prompt is displayed.



4. Confirm that you want to send account information to all users in the group. A message is displayed confirming that the email has been scheduled for sending. If the email fails to be delivered, check the **Alarms** pane on the **Diagnostics** page. See [Running Cisco TMSPE Diagnostics, page 49](#).

To send account information to any additional users added at a later date, if **Enable automatic email sending to imported users** is not enabled, notify the users individually as explained in [Sending Account Information to a Single User, page 28](#)

## Deploying Smart Scheduler

Smart Scheduler is a smart interface to Cisco TMS booking, using the Cisco TelePresence Management Suite Extension Booking API (Cisco TMSBA).

The layout is scalable and touch-screen friendly.

Smart Scheduler is a part of the Cisco Collaboration Meeting Rooms Hybrid solution, allowing users to set up telepresence meetings with and without WebEx.

Users can book:

- **Telepresence rooms**  
Any bookable system in Cisco TMS can be scheduled directly.
- **Call-in participants**  
Any system that is not supported by Cisco TMS booking can be scheduled as a call-in participant, including devices provisioned by Cisco TMSPE.  
Call-in participants must use the following protocols:

Protocol	Select
<b>ISDN</b>	Call-in participants must use ISDN for video or ISDN Audio
<b>IP(H323)</b>	Call-in participants must use IP(H323) for video or IP(H323) Audio
<b>SIP</b>	Call-in participants must use SIP for video or SIP Audio.

## Best Practices and Limitations

We strongly recommend that bookings created in Cisco TMS not be modified using Smart Scheduler, as this interface does not support all features and options that may have been chosen for the meeting in Cisco TMS.

Specifically:

- Exceptions to recurrent meeting series are not supported in Smart Scheduler. Any modification will be applied to all occurrences.
- Smart Scheduler will rename call-in participants added from Cisco TMS.

## Booking Limitations

The following limitations apply when booking through Cisco TMSPE or any other extension using Cisco TelePresence Management Suite Extension Booking API:

- Cascading to additional MCUs when the number of participants exceeds the capacity of the first MCU is not supported.  
To support such scenarios, set up Cisco TelePresence Conductor as the preferred MCU in Cisco TMS.

- When a service user is performing all bookings, the booking permissions are the same for all users. Individual permissions and restrictions in Cisco TMS are ignored.
- Meetings in the past cannot be changed or deleted, and you cannot move a meeting from the past to the future.
- If sufficient system licenses are not available at the time of editing an existing booking, the booking will be deleted.
- Yearly recurrence is not supported.
- When the Smart Scheduler is used, booking permissions for endpoints configured on Cisco TMS through Microsoft Outlook using Cisco TMS/ Cisco TMSXE combination, works in the expected manner. However, permissions configured on Cisco TMS for video endpoints are not adhered, when booking is done using the Smart Scheduler.
- If WebEx is added via Smart Scheduler then Cisco Meeting Server will not be selected as a bridge.

### Booking Horizon and Recurrence

Cisco TMS will decline any meeting request that is not within its booking horizon or that has an unsupported recurrence pattern:

- Series with more than 100 occurrences or with no end date.
- Meetings including occurrences outside of the Cisco TMS booking window. We strongly recommend configuring identical booking windows for Cisco TMS and all integrated resource mailboxes in Exchange.
- Meetings in the past.

### Ongoing Meetings

Updating a single meeting that is currently ongoing is possible, but will not always be successful.

- Modifying any meeting, extending the meeting will fail if it creates a booking conflict for any of the participants.
- Modifying single meetings, including meetings that are part of a series:
  - Editing the start time will not work and Cisco TMS will throw an exception.
  - Editing the meeting so that it would be required to be disconnected and re-routed will not be successful. For example, if the meeting is using a bridge that does not support WebEx, you cannot add WebEx during the meeting.
  - Any other aspects of the meeting can be modified, but if the number of participants exceeds the available capacity of the MCU or TelePresence Server, Cisco TMS will throw an exception and the participants will not be added.
- *Deleting* a recurrent series while a meeting in the series is ongoing will cause the ongoing meeting to end.
- *Modifying* a recurrent series while a meeting in the series is ongoing will turn the ongoing occurrence into a single meeting, separate from the series:
  - Any occurrences of the modified series that are in conflict with the ongoing meeting, will not be created.
  - Any past occurrences in the series will not be modified.
  - Pending occurrences are assigned new conference IDs.

## User Access to Smart Scheduler

Users with the necessary credentials can reach Smart Scheduler immediately on:

**`http://<Cisco TMS server address>/tmsagent/tmsportal/#scheduler`**

Users who already use Cisco TMS can also click the portal icon in the upper right corner to go to Smart Scheduler and FindMe:



## Access Rights and Permissions

For the user to be able to access the Smart Scheduler, the permission must be set for the user .

1. Go to **Administrative Tools > User Administration > Groups >**.
2. Select **Group**.
3. Click **Set permissions**.
4. Go to **> Booking > Misc**.
5. Check **Booking**.

Access to Smart Scheduler works the same as access to Cisco TMS; users must have one of the following:

- A local account on the Cisco TMS Windows Server
- A domain account that the server trusts through Active Directory. By making the server a member of the domain, all trusted domain users can automatically use their existing Windows credentials.

A Cisco TMS user will be created for them when they access the site if it does not already exist.

Note that the actual booking is not created directly by the individual user, but on their behalf by the Cisco TMSPE service user added during installation. Booking permissions for individual systems will therefore be the same for all users, so that all users who can log in to the Smart Scheduler will be allowed to book all endpoints.

Do not use this service user to log onto Smart Scheduler and create bookings.

## Time Zone Display

Bookings will be created using the time zone detected on the user's computer. To see their time zone, users can go to the date and time settings in the User Portal, **Account Settings > Locale**. Note that as the detection works for time zone rule sets, but not names, the name displayed for the user's time zone may be incorrect.

The users can use this setting to set their preferred display format for time and date, which is stored within the Web Storage of the browser.

## WebEx Booking

With Smart Scheduler users can book:

- Cisco Collaboration Meeting Rooms Hybrid meetings—telepresence with WebEx.
- Telepresence-only meetings.

The option to include WebEx in a meeting will be available in the Smart Scheduler booking form if Cisco Collaboration Meeting Rooms Hybrid has been set up with Cisco TMS, see [Cisco Collaboration Meeting Rooms Hybrid Requirements, page 12](#).

We strongly recommend that Single Sign-On be deployed for Cisco TMS and WebEx for easy addition and management of users.

In a non-SSO scenario, a WebEx username and password must be manually added for each Cisco TMS/Smart Scheduler user that will book with WebEx. Administrators can add this in Cisco TMS, or users can add credentials themselves through the Smart Scheduler settings.



## How Smart Scheduler Works

1. When a domain user signs into Smart Scheduler and books a meeting, the request is passed to Cisco TMS.
2. This communication goes through the Cisco TelePresence Management Suite Extension Booking API (Cisco TMSBA).
3. The Cisco TMS user entered during installation of Cisco TMSPE is the service user for Smart Scheduler. This user creates the booking in Cisco TMS on behalf of the Cisco TMSPE user. If the Cisco TMSPE user does not already exist in Cisco TMS, it will be created at the same time as the booking.
4. When the booking is complete, Cisco TMS sends an email confirmation to the user who booked the meeting. The message containing meeting details including route, scheduled systems, WebEx information, and so on, may then be forwarded to the other meeting participants.

Cisco TMS also sends email to the service user for Smart Scheduler when a booking is created or updated. For more information on the service user and how to set it up not to receive email, see [Cisco TMS username and password, page 13](#).

## Deploying Collaboration Meeting Rooms

### What are Collaboration Meeting Rooms?

Collaboration Meeting Rooms (CMRs) are reserved virtual spaces that have a set video address. Users can call in to that address at any time to start a meeting.

Collaboration Meeting Rooms provide an easy way to connect using telepresence without knowing where other participants are located; everyone dials into the same virtual room from their laptop, telepresence room, desktop endpoint, or their phone.

### Room Size and Quality

As with other meeting rooms, Collaboration Meeting Rooms can vary in capacity and available resources.

As an administrator, you will be able to determine:

- the maximum number of participants available for the rooms
- the video quality users can expect for their rooms
- how long meetings in rooms may last

Users can view these properties when they access their Collaboration Meeting Room portal page. Room owners decide on the video layout, and they can modify the name of the room, which appears as a banner that welcomes participants when they call in to the room.

### PIN Protection

Access to rooms can be restricted by the use of PIN codes. The administrator determines whether a PIN is required for host and/or guests, and the minimum number of digits.

Note that changing the PIN requirements for CMRs after initial setup is likely to cause confusion for users. We strongly recommend that you notify users when making changes of this nature.

See also [Making Changes that Affect Collaboration Meeting Rooms, page 42](#) and [Setting up Host and Guest Roles in CMRs, page 40](#).

## How Collaboration Meeting Rooms Are Created

Creating Collaboration Meeting Rooms requires a deployment of TelePresence Conductor with Unified CM or Cisco VCS, configured with one or more bridge pools and Service Preferences.

In Cisco TMSPE, the administrator:

- Sets up a user base with one or more groups of users in that will be allowed to create their own Collaboration Meeting Room.
- Creates one or more CMR templates linked to Service Preferences on TelePresence Conductor. A group's CMR template determines the address pattern and available parameters for each user's CMR.
- Applies required template to groups. You can only apply one template per group.

When notified by the administrator that the CMR service is available, each user can initiate the creation of their own CMR on their TelePresence User Portal page. Depending on the CMR template, this creates an alphanumeric and/or a numeric video address for each user's CMR on TelePresence Conductor.

The CMR is now permanently available and can be accessed at any time.

## Differences from TelePresence Conductor-created Conferences

A CMR is a conference on TelePresence Conductor that has been created by Cisco TMSPE.

A CMR template in Cisco TMSPE corresponds to a conference template *and* a conference alias on TelePresence Conductor.

Beware that:

- Collaboration Meeting Room created using Cisco TMSPE cannot be modified in TelePresence Conductor.
- Conferences templates and aliases created in TelePresence Conductor cannot be modified in Cisco TMSPE.
- The "lecture" conference type is not supported with Collaboration Meeting Rooms.

## Collaboration Meeting Room Resource Consumption

When you provision a CMR on TelePresence Conductor using Cisco TMSPE, TelePresence Conductor reserves the resources for one participant with the defined quality level. When participants dial into the CMR and resource optimization is enabled, TelePresence Conductor optimizes the resources so that only the resources that are required are used on the conference bridge.

However, the resources that were previously reserved are not freed up completely. The resources can be used by additional participants dialing into the same CMR. But the reserved resources cannot be used for other conferences. The conference bridge utilization on TelePresence Conductor shows the number of resources reserved if this number is higher than the number of resources used.

## Setting up Collaboration Meeting Room

### Before You Start

Cisco TMSPE must be set up and enabled as described in this document:

- You must install and enable the application, see [Installing Cisco TMSPE, page 18](#).
- You must have set up a user base, see [Creating Groups and Adding Users, page 22](#).

TelePresence Conductor must be set up with one or more populated bridge pools and one or more Service Preferences:

- Follow the instructions in [Cisco TelePresence Conductor with Unified CM Deployment Guide](#).
  - Omit the tasks to create conference templates, aliases, and auto-dialled participants on TelePresence Conductor, as you will perform corresponding tasks on Cisco TMSPE instead.
  - To support users creating auto-connected participants, ensure that you correctly configure the rendezvous location: **Conference configuration > Locations > Select location > SIP trunk setting for out-dial calls**.
- The only supported bridge types are Cisco TelePresence Server and Cisco TelePresence MCU Series.

## Connecting to TelePresence Conductor

You can add a maximum of 30 TelePresence Conductor connections to Cisco TMSPE.

Connect only to one TelePresence Conductor from a cluster.

On each TelePresence Conductor to be connected with Cisco TMSPE:

1. Go to **Users > Administrator accounts**.
2. Click **New**.
3. Add a new user exclusively for Collaboration Meeting Rooms, with the following settings:
  - **Access level:** *Read-write*
  - **Web access:** *No*
  - **API access:** *Yes*
  - **State:** *Enabled*
4. Click **Save**.

In Cisco TMS:

1. Go to **Systems > Provisioning > Users**.
2. Under **Collaboration Meeting Room Templates**, click **TelePresence Conductor Settings**.  
The **TelePresence Conductor Settings** dialog appears.
3. Click **Add New**.  
The **TelePresence Conductor Configuration** dialog box appears.
4. Fill in the credentials you created for TelePresence Conductor.

Field	Description
<b>Hostname/IP</b>	The hostname or IP address of the TelePresence Conductor you want to connect to.
<b>Port</b>	The port to connect on. By default, the connection uses HTTPS on port 443.
<b>Username</b>	The credentials for a TelePresence Conductor administrator account with the following settings and permissions: <ul style="list-style-type: none"> <li>– <b>Access level:</b> <i>Read-write</i></li> <li>– <b>Web access:</b> <i>No</i></li> <li>– <b>API access:</b> <i>Yes</i></li> <li>– <b>State:</b> <i>Enabled</i></li> </ul>
<b>Password</b>	
<b>Domain</b>	The domain that this TelePresence Conductor will append for all numeric aliases created through Cisco TMSPE.

5. Click **Connect**.
  - If connection is successful, you will be returned to the **Manage Conductors** dialog, where the newly added TelePresence Conductor is visible in the list. Click the X to close, unless you need to add another TelePresence Conductor.
  - If there is a problem with the connection, you will be returned to the **Conductor Configuration** dialog so that you can make any necessary adjustments to the settings.

## Creating Templates

Settings for Collaboration Meeting Room must be configured on a per-group level. The settings are configured by assigning templates to groups.

To create a template:

1. Go to **Collaboration Meeting Room Templates**.
2. Click **New Template**.

## 3. Fill in the settings:

**Table 1 Collaboration Meeting Room template configuration fields**

Field	Description
<b>Template Name</b>	<p>Assign a descriptive name to each template to ease the selection and maintenance of templates as the list grows.</p> <p>For example, include a descriptor for video quality, geographical location, or other signifier that clearly conveys what the template does.</p>
<b>TelePresence Conductor</b>	Select the TelePresence Conductor to use with the template from the drop-down list.
<b>Service Preference</b>	Select a Service Preference that has already been created on TelePresence Conductor.
<b>SIP Alias Pattern</b>	<p>Create a pattern for alphanumeric dialing if supported by your Unified CM deployment. The pattern must match your dial plan.</p> <p>For example:</p> <pre>{username}@meeting.example.com</pre> <p>The recommended variables are:</p> <ul style="list-style-type: none"> <li>- {username}</li> <li>- {email}</li> <li>- {office_phone}</li> <li>- {mobile_phone}</li> </ul> <p>{display_name}, {first_name}, and {last_name} are also supported variables, but will typically lead to conflict during room creation in organizations where many may share the same name.</p> <p>We strongly recommend using a unique identifier to minimize the risk of conflict and ensure alias predictability for users.</p> <p>In the event of alias conflict when a user creates a new room, Cisco TMSPE will create a numeric alias only if enabled, or fail to create a room if no aliases can be generated.</p>
<b>Numeric Alias Pattern</b>	<p>Whether to add a numeric alias for each room in addition to the alphanumeric alias.</p> <p>The selected pattern must match the dial plan of your call control device.</p> <p>Check to display the below settings.</p>
<b>Type</b>	<p>Select whether to base the numeric alias pattern on:</p> <ul style="list-style-type: none"> <li>- number ranges (<i>Generate a Number</i>) .</li> <li>- a RegEx pattern (<i>Office Phone</i> or <i>Mobile Phone</i>).</li> </ul>

**Table 1 Collaboration Meeting Room template configuration fields (continued)**

Field	Description
<b>Number Ranges</b>	<p>Enter one or more number ranges to use for the numeric aliases. Ranges must be written with a hyphen and no spaces, and multiple ranges must be separated by commas.</p> <p>Note that:</p> <ul style="list-style-type: none"> <li>Both parts of the range must contain the same number of digits. For example, 01–99 will work, but 1–99 will not.</li> <li>Ranges may overlap within and across templates. Duplicate numbers will not be generated.</li> <li>Numbers will be assigned randomly within the range, but if there are multiple ranges, the ranges will be consumed sequentially.</li> <li>A single number range cannot span more than one million numbers.</li> </ul> <p>Example: 100000–123456, 200000–234567</p>
<b>Prefix</b>	Enter a string of numbers that will constitute the first part of all numeric aliases.
<b>RegEx</b>	<p>To create the last part of the numeric alias, you may opt to use the user's office phone number or mobile phone number. Either choice requires that each user has the specified type of phone number available in Active Directory.</p> <p>Use the RegEx field to specify which part or parts to extract from the phone number.</p> <p>Keep in mind that using parts of a phone number will not always generate a unique number.</p> <p>We strongly recommend using a unique identifier to minimize the risk of conflict and ensure alias predictability for users.</p> <p>In the event of alias conflict when a user creates a new room, Cisco TMSPE will create an alphanumeric alias if a pattern exists, or fail to create a Collaboration Meeting Room if no aliases can be generated.</p> <p><b>Example:</b></p> <p>If the regex result contains one or more match groups, the result will be all match groups concatenated. If there are no match groups, the result will be the entire match result.</p> <p>In this example we will match against the phone number 123.456.7890.</p> <ul style="list-style-type: none"> <li>Given the regex <code>\d{4}</code> which will match the last four digits without any capture groups. The result will be 7890.</li> <li>Given the regex <code>(\d{3})\.\d{4}</code> which will match 456.7890 but also has one match groups which matches 456. The result will be 456.</li> <li>Given the regex <code>((?&lt;=\.\d)\d{2}(?=\.)) (?:\.)(\d{4})</code> which will match 56.7890 with two match groups 56 and 7890. The result will be 567890.</li> </ul>
<b>Maximum Conference Quality</b>	From the range of available video qualities, select the maximum quality that users will have access to when you assign them this template.
<b>Content Sharing</b>	Whether to allow content (presentation) sharing in rooms based on this template.

Table 1 Collaboration Meeting Room template configuration fields (continued)

Field	Description
<b>Maximum Content Quality</b>	<p>From the range of available qualities for content (presentation) sharing, select the maximum quality that users will have access to.</p> <p>The <b>Maximum Content Quality</b> setting is not applicable to CMRs that are hosted on MCU.</p>
<b>Minimum Host PIN Length</b>	<p>These settings control the requirements and options for PIN protection of CMRs based on the template:</p> <ul style="list-style-type: none"> <li>First, enter the minimum number of digits for the host role's PIN in <b>Minimum Host PIN Length</b>. If you leave the setting as 0, the CMR owner is not required to use a PIN for any participants.</li> </ul>
<b>Allow Guest Role</b>	<ul style="list-style-type: none"> <li>Select whether to allow the role of guest for CMRs based on this template.: <ul style="list-style-type: none"> <li>The guest role has more limited privileges than the host role.</li> <li>If <b>Allow Guest Role</b> is disabled, all participants will have the same privileges and PIN requirements as the host.</li> </ul> </li> </ul>
<b>Minimum Guest PIN Length</b>	<ul style="list-style-type: none"> <li>If <b>Allow Guest Role</b> is enabled: <ul style="list-style-type: none"> <li>Enter the minimum number of digits for the guest PIN in <b>Minimum Guest PIN Length</b>. If you leave the setting as 0, the CMR owner is not required to use a PIN for the guest role.</li> </ul> </li> </ul>
<b>Guest Lobby</b>	<ul style="list-style-type: none"> <li>Choose whether to enable <b>Guest Lobby</b>, which means guests must wait in the lobby unless at least one host is present in the CMR.</li> </ul> <p>For more information, see <a href="#">Setting up Host and Guest Roles in CMRs, page 40</a>.</p>
<b>Limit Number of Participants</b>	Choose whether to set a maximum number of participants that will be allowed in the Collaboration Meeting Room.
<b>Maximum Participants</b>	<p>Set a maximum number of participants to allow if <b>Limit Number of Participants</b> is enabled.</p> <p>The upper limit for number of participants allowed in a CMR is controlled by Cisco TelePresence Conductor. For more detail, see documentation for <a href="#">Cisco TelePresence Conductor</a>.</p>
<b>Limit Conference Duration</b>	<p>Choose whether to set a maximum duration for meetings in the CMR.</p> <p>Enable this setting to prevent meetings where participants forget to disconnect, so that the meeting continues.</p>
<b>Maximum Minutes</b>	Set a maximum meeting duration in minutes if <b>Limit Conference Duration</b> is enabled.
<b>Allow Multiscreen</b>	Choose whether to allow participating telepresence systems to use more than one screen.
<b>Maximum Screens</b>	Set a maximum number of screens allowed per participant if <b>Allow Multiscreen</b> is enabled.

**Table 1 Collaboration Meeting Room template configuration fields (continued)**

Field	Description
<b>Allow Cascading</b>	Choose whether to allow the user of this CMR to seamlessly expand an ongoing meeting if there is an available bridge in your environment. This requires reserving one or more bridge ports or connections for cascading, which will always be available to the CMRs defined by this template.
<b>Number of Cascades</b>	Set a number of MCU ports or TelePresence Server connections to reserve for cascading if enabled.
<b>Optimize Resources</b>	Select whether to allow TelePresence Conductor to free up any allocated resources not used by participants once the meeting has started. This setting is enabled by default.
<b>Include WebEx</b>	If CMR Hybrid is deployed, choose whether to enable the creation of instant WebEx meetings connected to the CMR.  For this option to work, you must first go to <b>Administrative Tools &gt; Configuration &gt; Provisioning Extension Settings &gt; Collaboration Meeting Room</b> and set <b>Allow WebEx Connections</b> to <b>Yes</b> .
<b>Advanced Parameters</b>	Configure bridge-specific JSON objects for advanced conference parameters on creation.  For examples of JSON, see <a href="#">Cisco TelePresence Conductor Administrator Guide</a> .

4. Click **Save**.

## Applying Templates to Groups

In Cisco TMS:

1. In **Systems > Provisioning > Users**, go to the group to which you want the template applied.
2. Select the radio button for the template you want in the **Active** column.

The template will be applied immediately and a notification will be displayed.

All users in the group can now create their own Collaboration Meeting Room.

Users may control the following:

- whether to use a PIN, if you have not specified this as a requirement
- what their room PIN will be, within the limitations you specify
- a banner that is displayed when meeting attendees join their room

## CMR Count

The number of rooms created with each template will be displayed in the Count column in the list of templates. Note that this count is the total for the template, regardless of which group is currently selected.

## Setting up Host and Guest Roles in CMRs

When creating a template for Collaboration Meeting Rooms, the administrator can choose whether or not the CMR owner will be able to distinguish between host and guest participants.

## Host Privileges

The participant or participants connecting to a CMR as a host can connect at any time regardless of whether there are other participants in the room.



A PIN may be required for them to join, depending on the configurations made by the administrator and the CMR owner. Depending on the bridge used, participants connecting as guests may be required to wait until a host joins the meeting before they will be allowed into the CMR.

- Cisco TelePresence MCU Series: guests must always wait for a host to join.
- TelePresence Server: the policy is determined by the **Guest Lobby** setting of the CMR.

## Allowing the Guest Role

On the template of the CMR:

- Check **Allow Guest Role**.  
To make the guest role optional to CMR owners, you must leave the host PIN requirement as 0 (optional).
- Select whether to enable **Guest Lobby**, which means guests must wait in the lobby unless at least one host is present in the CMR. When a conference is initiated, automatic dial out is initiated for all the favorite endpoints that are part of the conference. In this case, the favorite participant will join the conference first and then subsequently all the remaining participants in the lobby will join the conference.  
This setting will apply to all rooms based on the template and is not configurable for the CMR owner.

When the guest role is allowed:

- The guest role will only be used if the administrator or CMR owner set a PIN requirement for the host. If no PIN is set for the host, everyone is allowed into the CMR automatically with host permissions.
- If a PIN is set for the host, but not for the guests, guests will be asked to press # to connect to the CMR.
- You can only have a PIN requirement for the guest if there is also a PIN requirement for the host.

## Disallowing the Guest Role

To make all participants have the same PIN requirements and the same privileges, uncheck **Allow Guest Role** on the CMR template.

When the guest role is not allowed, all participants are treated as hosts and can connect at any time regardless of whether there are other participants in the room.

## Including WebEx Participants in CMR meetings

If you have deployed CMR Hybrid, you can include WebEx in CMRs so that users may connect using either telepresence or WebEx.

When enabled through the Collaboration Meeting Room template, a **Create WebEx Connection** button will appear on each user's CMR page on the TelePresence User Portal. The button allows the user to create a temporary WebEx connection for their CMR.

As the connection is temporary and will eventually time out, the portal page advises users to create the connection and distribute the WebEx details shortly before the meeting starts.

## Before you start

Before you can enable WebEx in CMRs:

- CMR Hybrid must be deployed. See [Cisco Collaboration Meeting Rooms Hybrid Configuration Guide](#) for details and instructions.
- The owner of each CMR must be a registered WebEx user associated with a current WebEx site with their own username and password. Otherwise, the **Create WebEx Connection** button will not appear for the user.
- If planning to change an existing template, read [Making Changes that Affect Collaboration Meeting Rooms](#), page 42

- To prevent potential toll fraud issues, we recommend disabling **Call-back teleconferencing** on the WebEx site that is used for CMRs.

## Enabling WebEx in CMRs

You must enable WebEx for CMR before you can include the feature in one or more templates:

1. In Cisco TMS, go to **Administrative Tools > Configuration > Provisioning Extension Settings**.
2. Under **Collaboration Meeting Room**, set **Allow WebEx Connections** to *Yes*.
3. Go to **Systems > Provisioning > Users**.
4. Select an existing template for editing or create a new template.
5. Check **Include WebEx**.
6. Click **Save**.
7. Click **Regenerate CMRs**.

## Making Changes that Affect Collaboration Meeting Rooms

Several administrator operations will cause changes to Collaboration Meeting Rooms when made. We strongly recommend that administrators fine-tune templates as much as possible before applying them to groups and allowing users to create their CMR.

When you need to make changes to templates after making Collaboration Meeting Rooms available to users, plan the changes and minimize disruption to users by following these best practices:

- Schedule a maintenance window and make it off-hours and/or announce it to users so they can avoid creating or modifying their CMR during maintenance.
- During planning, find out how each intended change will affect existing rooms, and let users know what to expect if the change is significant.

## Modifying or Replacing the Template for a Group

The following actions will impact the available settings for Collaboration Meeting Room in the affected groups:

- Selecting a different template for a group.
- Making changes to a template that has already been assigned to a group, by modifying settings or changing the Service Preference.

Setting the CMR template to *None* for any group will remove the entitlement to create and maintain a CMR for all users in that group.

Movement of a user between groups or changing user filters must be done carefully as the sequence or steps performed might lead to the deletion of CMR.

- When a user is moved to different group and no template is assigned, this leads to deletion of CMR in database.
- When a user is moved to different group with same template, then CMR's are retained.
- When a user is moved to different group with a new template then the CMR has details based on new template.

When changing a template the **SIP Alias Pattern** will always regenerate. The **Numeric Alias Pattern** never regenerates once it is set on a CMR.

To edit any template:

1. Click the pencil icon next to the template name in the CMR template list.
2. Modify template settings as required.
3. Click **Save**.

4. Repeat the previous steps for any other templates that need modifying.
5. When all template changes are completed, the counter next to the **Check sync status** button will let you know how many rooms are currently out of sync with the modified templates. Click the **Regenerate CMRs** button to synchronize.

### Changing the PIN Policy

- If you make the PIN policy stricter, Cisco TMSPE will generate a new PIN for any non-compliant rooms when the changes are synchronized.

**Note:** If you set a stricter PIN policy, PINs are generated for all CMRs that do not meet the new criteria. Notify users that their PIN may have changed and that they must log into the portal to change their PIN.

- If you make the PIN policy less strict, existing rooms will not be affected.

### Deleting Templates

Click the red deletion icon next to the template name in the CMR template list to delete.

Note that it is not possible to delete a template as long as it is associated with existing rooms.

### Deleting Users

When a user is removed from the user repository, the user's CMR will be deleted automatically.

### Moving Users Between Groups

When a user's group changes in the user repository, normally due to changes in Active Directory, their assigned CMR template will also change if their new group has a different template.

When a non Active Directory user is moved between groups having different templates, a new room for that user is created and it usually takes around 15 to 20 minutes to be created. After the room is created, the user has to regenerate the Collaboration Meeting Room to sync the room with that template and also to have the changes reflected on the Cisco TelePresence Conductor.

Refer to [Modifying or Replacing the Template for a Group](#), for more information about how users are moved between groups and templates are modified or replaced.

1. Cisco TMSPE will register the change during the next health check. The **Run Health Check** can also be initiated manually from the **Provisioning Extension Diagnostics** page.
2. The CMR of the user will be displayed as out of sync. To synchronize, click **Regenerate CMRs** on the **Collaboration Meeting Room Templates** page to have the change reflected on the Cisco TelePresence Conductor.

### Touch Tones and DTMF

Users can enter touch tones for auto-connections.

1. Go to **New Favorite**, use the **Video Address or Number** field.
2. Enter '\*' between the number and the touch tone digits.
3. Use a comma ',' for a 1 second pause. (for example 18005551212\*\*123456#,,1234#)
4. Select **Auto-connection**.
5. Click **Save**

## Auto-connected Participants

Users can use the **Favorites** feature to add a recording alias as an auto-connected participant that will be connected whenever a new meeting is initiated in the CMR.

Auto-connected participants can also be used for adding other participants in support of different scenarios, such as:

- The user's own endpoint- to avoid the user having to wait in their own meeting for others to join.
- An IPVCR (or alternative playback device) to play back a recording.
- An audio bridge. To have a parallel video and audio conference, this can be used to trigger the cascade.
- A single alias that quickly brings together a team of people for an emergency meeting.

## Add a Favorite Auto-connected Participant

To add a favorite auto-connected participant, perform the steps given below:

1. Go to CMR user portal.
2. Click **Auto-connected participant**
3. Click **Favorites**
4. Click **New Favorite**.
5. Enter the information about the participant.
6. Click **Save**.
7. Click **Back**.

## Modify a Favorite Auto-connected Participant

To modify a favorite auto-connected participant, perform the steps given below:

1. Uncheck the box next to favorite participant
2. Click on **Favorites**
3. Click the **Edit** button on the right next to the favorite you want to edit.
4. Edit the value that needs to be changed
5. Click **Save**
6. Click **Back**. The modified favorite is displayed

## Maintaining Users

This section describes maintenance tasks you may need to perform after setting up Cisco TMSPE.

### Synchronizing User Data

When you configure the import of user account data from external sources (see [Creating Groups and Adding Users, page 22](#)), Cisco TMSPE uses the information you supply to set up a synchronization schedule. Synchronization takes place once a day. You cannot change the schedule, but you can run a manual synchronization at any time. (See [Running a Manual Synchronization, page 46](#).)

LDAP implementations other than Active Directory must have the following for import and synchronization to be supported:

- An `entryUUID` field as defined by [RFC 4530](#).
- Simple paging as defined by [RFC 2696](#).

### Mapping of LDAP and AD Fields

The table below shows the way in which user attributes from external Active Directory or LDAP sources are mapped to Cisco TMSPE when you import and synchronize user data. Other fields, including Active Directory and LDAP passwords, are not imported or synchronized.

The **Cisco TMSPE User Attribute** column shows the names of user attributes to which external directory attributes are mapped. You can include these user attributes in template patterns. The following example includes the `username` attribute in a video address pattern:

```
{username}@example.com
```

Some user attributes can only be used to define certain specific patterns. For example, you cannot include the `username` attribute in the Caller ID pattern. For further information, view the Cisco TMSPE online help.

From Active Directory	From LDAP	To Cisco TMSPE	Cisco TMSPE User Attribute
<code>objectGUID</code>	<code>entryUUID</code>	<code>external_id</code>	
<code>sAMAccountName</code>	<code>cn</code>	<code>Username</code>	<code>username</code>
<code>mail</code>	<code>mail</code>	<code>Email</code>	<code>email</code>
<code>title</code>	<code>title</code>	<code>Title</code>	
<code>givenName</code>	<code>givenName</code>	<code>First Name</code>	<code>first_name</code>
<code>sn</code>	<code>sn</code>	<code>Last Name</code>	<code>last_name</code>
<code>company</code>	<code>company</code>	<code>Company</code>	
<code>department</code>	<code>department</code>	<code>Department</code>	
<code>telephoneNumber</code>	<code>telephoneNumber</code>	<code>Office Phone</code>	<code>office_phone</code>
<code>mobile</code>	<code>mobile</code>	<code>Mobile Phone</code>	<code>mobile_phone</code>
<code>displayName</code>	<code>displayName</code>	<code>Display Name</code>	<code>display_name</code>

### Testing a Manual Synchronization

To test and preview the results of running a manual synchronization:

1. In Cisco TMS, go to **Systems > Provisioning > Users**.
2. In the **Users and Groups** container, navigate to and click the group you want to test. Information about the selected group is displayed in a number of panes.
3. In the **User Import** pane, click **Test import**.  
Information is displayed in the **User Import** pane to indicate that the test is in progress. When the test has finished running, information confirms whether or not the test finished successfully. The total number of processed records is displayed, as well as the number of records that would be created, updated, moved, or deleted by a manual synchronization.

## Running a Manual Synchronization

To run a manual synchronization:

1. In Cisco TMS, go to **Systems > Provisioning > Users**.
2. In the **Users and Groups** container, navigate to and click the group you want to synchronize. Information about the selected group is displayed in a number of panes.
3. In the **User Import** pane, click **Start import**.

## Moving Users and Groups

To move groups and manually created accounts:

1. In Cisco TMS, go to **Systems > Provisioning > Users**.
2. In the **Users and Groups** container, navigate to and click the group or user you want to move. Information about the selected group is displayed in a number of panes.
3. Above the **User Settings** pane, click **Move User** or **Move Group**.
4. In the **Move** dialog box, navigate to and click the target user or group, and then click **Move**.

## Moving User Accounts Imported from External Sources

To move users from external sources, you need to change the import filters of the group into which the user is currently imported, and the target group into which you want the user to be imported. Change the filter in the current group so that the user is excluded, and apply a filter in the target group so that the user is included.

## Searching for User Accounts

To search for a user account:

1. In Cisco TMS, go to **Systems > Provisioning > Users**.
2. In the search field below the heading of the **Users and Groups** container, enter the display name of the user account you want to find.  
You can enter a partial search string. User accounts that match the search string are displayed in the **Users and Groups** container.
3. To display details of a matching user account, click the account.
4. To identify the group to which the account belongs, click the **Go to group** button localized on top of the left pane.

## Renaming Groups and User Accounts

You can change the display name of groups and manually created users. Note that you cannot change the display name of users imported from external directories.

To change the display name of users and groups:

1. In Cisco TMS, go to **Systems > Provisioning > Users**.
2. In the **Users and Groups** container, navigate to and click the group or user whose display name you want to change.  
Information about the selected group is displayed in a number of panes.

**example\_group**

Rename Group... Delete Send Account Information Move Group Toggle Details

### User Settings

Name	Pattern	Origin
Video Address Pattern	{first_name}-{last_name}@example.com	example_group
Caller ID Pattern	{mobile_phone}	example_group
Device Address Pattern	{username}-{device.model}@example.com	example_group
Image URL Pattern		root

Edit Reload

3. Above the **User Settings** pane, click **Edit User...** or **Rename Group...**. The corresponding dialog box appears.

### User Settings

Name	Pattern	Origin
Video Address Pattern	{first_name}-{last_name}@example.com	example_group
Caller ID Pattern	{mobile_phone}	example_group
Device Address Pattern	{username}-{device.model}@example.com	example_group
Image URL Pattern		root

Edit Reload

### Rename Group

Display Name:

Save Cancel

4. In the **Edit User** or **Rename Group** dialog box, enter the new name, and then click **Save**.

## Updating Cisco TMS Connection Details

To update connection details for Cisco TMS:

1. Go to **Administrative Tools > Configuration > Provisioning Extension Settings**.
2. Scroll to the **Cisco TMS Connection** section.

### Cisco TMS Connection

HTTPS \* ☒ Yes ☐ No

Connection Timeout \*  (seconds)

Receive Timeout \*  (seconds)

Username \*

Password \*

Save Cancel Restore Default

3. Modify settings as desired.
4. Click **Save**.
5. Restart the Provisioning Extension service, see [Restarting the TMS Provisioning Extension Windows Service](#), page 50.

## Maintaining the Databases

Cisco TMSPE uses three databases; **tmspe**, **tmspe\_vmr** and **tms\_userportal**. These databases must be kept co-located with each other. One database must not be downgraded or otherwise modified without the others.

## Backing up the Databases

We recommend backing up the Cisco TMSPE databases regularly.

## Moving or Renaming the Databases

After moving the databases, you must update the database settings in Cisco TMS Tools:

1. On the Cisco TMS server, go to **Start > Cisco TelePresence Management Suite > TMS Tools**.
2. Go to **Configuration > Cisco TMSPE Database Connection**.
3. Update the **Database Server\Instance** with the new location.
4. Update or verify the **Database Name**.
5. Verify the **Username**.
6. Enter the **Password** for the above user.
7. Click **OK**.

With a redundant Cisco TMS deployment, the above steps must be repeated on both servers.

After updating the database instance, restart the Windows service for the connection settings change to take effect, see [Restarting the TMS Provisioning Extension Windows Service, page 50](#) for instructions.



## Troubleshooting

This section describes the Cisco TMSPE built-in diagnostic tools and describes troubleshooting scenarios and strategies.

### Running Cisco TMSPE Diagnostics

Cisco TMSPE runs a regular health check every 30 minutes, and displays problems encountered in a list of alarms available in Cisco TMS at **Administrative Tools > Diagnostics > Provisioning Extension Diagnostics**. The health check monitors all services (for example, user repository, user preference, and phone book), and underlying resources such as database connectivity and internal messaging communications.

Additional system monitoring takes place every 10 minutes and reports issues such as low disk space and high system memory usage.

Diagnostics problems detected during a health check or as a result of system monitoring are displayed in the **Alarms** pane.

Information displayed on the **Provisioning Extension Diagnostics** page is not refreshed automatically. To update the information, reload the page.

Run Health Check Version: 1.2.0.24

Alarms					
Source IP	Source Name	Severity	Description	Last Reported	Detail
10.47.40.105	CMR	WARNING	Rooms are out of sync with conductor	05/6/2014 12:06:32 (W. Europe Daylight Time)	

System Status					
Service	Status	User Import	Device Import	Cleanup	Actions
User Repository					Cleanup
Device Repository					Cleanup
User Preference					Cleanup User Import
Phone Book					Cleanup
FindMe					Cleanup User Import Device Import
Diagnostics					Cleanup
CMR					

### Running a health check

To trigger a health check at any time:

1. In Cisco TMS, go to **Administrative Tools > Provisioning Extension Diagnostics**.
2. Above the **Alarms** pane, click **Run Health Check**.  
A message is displayed when the health check has completed. Any new alarms are displayed in the **Alarms** pane.
3. Click the icon in the **Details** column to view a description of the issue and suggestions for corrective actions in the **Alarm Detail** dialog box.
4. Complete one of the following actions:
  - Acknowledge the problem and remove it from the **Alarms** pane by clicking **Acknowledge**.
  - Keep the item in the **Alarms** pane by clicking **Cancel**.

### Viewing system status

The services that contribute to the provisioning extension solution are monitored regularly to determine their current status.

To view system status and take remedial action:

1. On the **Provisioning Extension Diagnostics** page, scroll down to the **System Status** pane.
2. View the following color-coded status circles:
  - Red circles indicate an error or warning.
  - Gray circles indicate 'No status Available'.
  - Green circles indicate Successful status.
3. To attempt to fix a problem or to update the status of a service, click the corresponding button:
  - System Status: click **Cleanup**.  
This action cleans up the delta table in the database, which holds information about data changes such as user and group updates. The accumulation of changes in the delta table can cause the database to grow over time.
  - User Import Status: click **User Import**.  
This action initiates a full import from the user repository to the target service.
  - Device Import Status: click **Device Import**.  
This action initiates a full import from the device repository to the target service.
4. View the Cleanup Status circle to confirm that the problem has been fixed.  
Typically, the status changes to orange indicating it is awaiting processing, to a cog wheel indicating that the task is in progress, to a green circle indicating that the status is now OK.

## Restarting the TMS Provisioning Extension Windows Service

In some error situations, restarting the Windows service may be necessary to allow Cisco TMSPE to resolve the problem. In certain scenarios this is also indicated as the "Corrective action" for an alarm on the **TMS Provisioning Extension Diagnostics** page.

To restart the service:

1. Open Server Manager.
2. Go to **Configuration > Services**.
3. Locate the TMS Provisioning Extension service and click **Restart**.

Note that initialization of the service may take 3-4 minutes, during which the Cisco TMSPE parts of Cisco TMS will be unavailable.

## Logs

### Cisco TMSPE and Cisco TMS Logs

To get a snapshot of all available logs for Cisco TMSPE and Cisco TMS:

1. Go to **Administrative Tools > TMS Server Maintenance**.
2. Click **Download Log Files**.

## Troubleshooting the Installation

### Checking the Installation Log

If problems occur during the installation of Cisco TMSPE to the Cisco TMS server, refer to the Cisco TMSPE Install Log. The Cisco TMSPE Install log can be found in:

`C:\Program Files (x86)\TANDBERG\TMS\TMSProvisioningExtension\app\logs`

This log is also included in the archive of logs provided when going to **Administrative Tools > TMS Server Maintenance** and clicking **Download Log Files**.

## Unable to Establish SQL Connection Through Java Runtime...

If you get this error while running the Cisco TMSPE installer, make sure your SQL Server Browser is in a running state. SQL Server Browser is used by the SQL client to resolve named instances and port numbers.

To view the SQL Server Browser and start it if necessary:

1. Open one of the following on your SQL server:
  - Go to SQL configuration manager and open SQL server services.
  - Go to **Computer Management > Services and Applications > Services**.
2. Locate the SQL Server Browser service and start it if it is not running.

If you opt not to start the service, you must provide a port number in the Cisco TMSPE installer. The only format supported for entering the port number is `<SERVER NAME>:<port number>`.

Note however that named instances by default use dynamic TCP ports, which would break the connection on reboot of the database server. We therefore strongly recommend keeping SQL Server Browser running.

## Unable to Find Valid Certification Path to Requested Target

If the Provisioning Extension Diagnostics show a red circle for the Phone Book service:

1. Click **Cleanup**.
2. After a few minutes, run a health check to refresh the information display.
3. If the circle is still red, check the log. If the `tmsprovisioningextension.log` file contains the following line:  
`Caused by: javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target`
  - a. Place your certificate file somewhere on the Cisco TMS server.
  - b. Update the JRE keystore from `JRE_HOME\bin` on the server using the following command:  
`keytool -import -alias myprivateroot -keystore ..\lib\security\cacerts -file c:\hello.cer`
  - c. Enter the password for the keystore when prompted. The default password is `changeit`.

## Portal Troubleshooting

### Cannot Access FindMe or Smart Scheduler

Error message: Access denied. Verify that all critical Windows Updates are installed on the server.

## Uninstalling Cisco TMSPE

There are two ways to uninstall Cisco TMSPE. The operation will be logged in different locations depending on your system configuration and the uninstallation method, as described below. No log data is deleted by uninstalling Cisco TMSPE.

## Using the Installer

1. Run the installer.
2. Follow the onscreen instructions to uninstall.

A log of the uninstallation will be created in:

`C:\Program Files(x86)\TANDBERG\TMS\wwwTMS\Data\Logs\Install.`

Note that starting the uninstallation process stops the Windows service, and that cancelling the uninstallation will not restart the service. See [Restarting the TMS Provisioning Extension Windows Service, page 50](#) for instructions.

## Using the Control Panel

1. Ensure the operation will be logged by following the instructions in the Microsoft Support article [How to enable Windows Installer logging](#)
2. Open the Add/Remove Programs list of the Windows Control Panel.
3. Locate Cisco TMS Provisioning Extension in the list and click **Remove**.

A log of the uninstallation will be created in the server's **Temp** folder. To access the log:

1. Go to **Start > Run**.
2. Type `%Temp%` and click **OK** to open the folder.
3. Look for a file name that starts with **MSI** and has the extension **.LOG**.

## Reusing or Replacing the Existing SQL Database When Reinstalling

Cisco TMSPE does not automatically delete the Cisco TMSPE SQL databases when uninstalling. The installer will detect existing Cisco TMSPE SQL databases, and you will be asked if you want to reuse the databases.

Use SQL Server Management Studio to remove the database. [SQL Server Management Studio](#) is included with Microsoft SQL Server 2012 and later versions.

## Appendix 1: Using Personal Multiparty Licensing with Cisco TMSPE

Two Personal Multiparty licenses are available:

- Personal Multiparty Basic (previously named Personal 4-Way Multiparty Conferencing) enables personal video conferencing for users who need to hold frequent impromptu discussions with small groups of colleagues.
- Personal Multiparty Advanced enables personal conferencing with as many participants as the conference bridge resources allow, hosted by a named user.

Both licenses cover:

- Collaboration Meeting Rooms provisioned by Cisco TMSPE/rendezvous conferences on Cisco TelePresence Conductor
- Ad hoc conferences on TelePresence Conductor

## Limitations

These licenses only apply to:

- Unified CM-based deployments—Cisco VCS-based deployments are not supported.
- TelePresence Server-hosted conferences—MCUs are not supported.

## Combining Licenses

You can mix Personal Multiparty licensing with Screen licensing if using separate conference bridges and pools. See [Cisco TelePresence Conductor with Cisco Unified CM Deployment Guide \(XC2.4\)](#) for instructions.

Both types of Personal Multiparty licenses can also share conference bridges and pools on the same TelePresence Conductor, if desired.

## Feature Support

**Table 2 Differences between Personal Multiparty Basic and Personal Multiparty Advanced**

	Personal Multiparty Basic	Personal Multiparty Advanced
<b>Collaboration Meeting Rooms provisioned by Cisco TMSPE/Rendezvous conferences in TelePresence Conductor</b>	Yes	Yes
<b>Ad hoc escalated conferences</b>	Yes	Yes
<b>TelePresence Conductor scheduling in Cisco TMS</b>	Not currently supported	
<b>Maximum conference size</b>	Up to 4 participants	Limited by the conference bridge capacity, concurrent usage, and the deployment's total number of Screen licenses included in Personal Multiparty Advanced license packs.
<b>Number of concurrent conferences per named host</b>	1	1
<b>Requirement that host is present in the conference</b>	Yes	Yes
<b>Maximum video resolution</b>	HD (720p 30fps)	Limited only by conference bridge capabilities
<b>Maximum content quality</b>	1280 x 720p 5fps	Limited only by conference bridge capabilities
<b>Multiscreen support</b>	Only one screen of multiscreen endpoints is displayed	Yes

The restrictions listed in the table above are not enforced automatically, but must be configured on TelePresence Conductor and in the CMR template.

- Instructions for configuring CMR templates in Cisco TMSPE are provided below.
- To configure TelePresence Conductor ad hoc conferences to work with either license, see [Cisco TelePresence Conductor with Cisco Unified CM Deployment Guide \(XC2.4\)](#).

## Applying License Restrictions to CMR Templates

See [Setting up Collaboration Meeting Room, page 34](#) for instructions on configuring Cisco TMSPE for use with TelePresence Conductor and Collaboration Meeting Rooms.

Replace the task [Setting up Collaboration Meeting Room, page 34](#) with the following procedure to create a CMR template that complies with Personal Multiparty Basic or Personal Multiparty Advanced:

1. In Cisco TMS, go to **Systems > Provisioning > Users**.
2. Under Collaboration Meeting Room Templates, click **New Template**.
3. Give the template a name, and select the appropriate TelePresence Conductor.
4. Select a **Service Preference** that contains conference bridges of type TelePresence Server.
5. Create a SIP alias pattern. We strongly recommend basing the pattern on username, which is always unique, to avoid alias conflicts.

6. Select whether to also include a numeric alias pattern, that may be generated within one or more specified number ranges, or based on an office or mobile phone number.
7. If using Personal Multiparty Basic, configure the required restrictions (if using Personal Multiparty Advanced, proceed to step 8):
  - Set the **Maximum Conference Quality** to *HD (720p 30fps video, stereo audio)* or lower.
  - If enabling content sharing, set the **Maximum Content Quality** to *1280 x 720p 5fps* or lower.
  - Check **Limit Number of Participants** and set the maximum to 4.
  - Leave the **Allow Multiscreen** setting disabled.
8. Configure remaining settings as desired.
9. Click **Save**.

Before continuing to applying the template to one or more groups, make sure that you have imported all the desired users from Active Directory into the appropriate Cisco TMSPE folders. For import instructions, see [Importing users from external directories, page 22](#).

## Tracking the Number of Licenses Used

The **Rooms** column in the list of Collaboration Meeting Room templates displays an updated count of how many CMRs have been created based on each template across all groups.

In order to comply with EULA terms, the administrator must ensure that the number of CMRs/rendezvous conferences created does not exceed the number of licenses purchased.

For detail on license terms and acquiring an overview of available licenses, see the [Cisco Collaboration Meeting Rooms \(CMR\) Premises web page](#).

## Notices

### Accessibility Notice

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

You can find more information about Cisco accessibility here:

[www.cisco.com/web/about/responsibility/accessibility/index.html](http://www.cisco.com/web/about/responsibility/accessibility/index.html)

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation at: [www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html](http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html).

Subscribe to What's New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.



## 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 are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

© 2019 Cisco Systems, Inc. All rights reserved.

## Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://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. (1110R)

