



Cisco TelePresence Management Suite Provisioning Extension with Cisco VCS

Deployment Guide

Last Updated: April 2019

Cisco TMSPE 1.13

Cisco TMS 15.7

Cisco VCS/Expressway X8.10

TelePresence Conductor XC 4.3



Contents

Introduction	11
This Deployment Guide	11
Related Documents	11
Prerequisites and Recommendations	13
Estimating Your Deployment Size	13
Hardware Requirements	14
Regular Deployment and Cisco Business Edition 6000	14
Large Deployment	14
Recommended Hardware and Virtualization for Large Deployments	15
Cisco TMSPE server software and configuration requirements	16
SMTP server requirements	17
SQL Server software and permission requirements	17
Cisco VCS requirements	17
Cisco Collaboration Meeting Rooms Hybrid Requirements	18
Cisco TelePresence Conductor	18
Required security permissions	18
For installation	18
For operation	18
TLS Support	18
Information needed during installation	19
Cisco TMS username and password	19
Database information	19
Database location	19
Feature options during installing	19
User import requirements	20
Service account	20
Secure connection	20
Active Directory	20

LDAP	20
Browser requirements	20
Administrator interface	20
User portal	21
Licensing requirements	21
Best practices for deployment	22
Upgrade endpoints to the latest software	22
Automate user creation and management with AD/LDAP	22
Use secure communication	22
Synchronize time in Cisco VCS and Cisco TMS	22
Multiparty Licensing	22
Configuring Cisco VCS for Provisioning	23
Provisioning Within Your Network	23
Setting up DNS for the Cisco VCS	23
Installing the Device Provisioning Option Key	24
Enabling SIP	24
Configuring How Cisco VCS Handles Calls to Unknown IP Addresses	24
Adding Cisco VCS to Cisco TMS	25
Enabling Provisioning on the Cisco VCS	26
Setting up a Cluster Name	26
Enabling Presence on the Cisco VCS	26
Presence on VCS Control	27
Presence on VCS Expressway	27
Verifying Device Authentication	28
Installing Cisco TMSPE	29
Installing Cisco TMSPE with a Redundant Cisco TMS Setup	29
Upgrading from Previous Versions to Cisco TMSPE 1.13	29
High-level Workflow	29
Upgrading Cisco TMSPE	29
Performing a New Installation	30
Enabling Cisco TMSPE	30
Setting up Communication Between Cisco TMS and Cisco VCS	31
Setting up Users and Provisioning	35
Creating Groups and Adding Users	35
Setting up Groups	35
Importing users from external directories	35

Adding Users Manually	39
Creating Address Patterns	39
Address Pattern Types	39
Adding the Patterns	40
Example Patterns	41
Setting up Configurations for Provisioned Devices	42
Obtaining Template Schemas	42
Uploading the Schema to Cisco TMS	43
Adding Configuration Templates	44
Assigning Configuration Templates to Groups	47
Provisioning Phone Books	48
Creating and Configuring Provisioning Phone Book Sources	48
Associating Phone Book Access to Groups	49
Configuring and Sending Account Information	50
Configuring Email Settings	50
Sending Account Information to a Single User	52
Sending Account Information to All Users in a Group	52
Deploying Smart Scheduler	53
Best Practices and Limitations	54
Booking Limitations	54
User Access to Smart Scheduler	55
Access Rights and Permissions	56
Time Zone Display	56
WebEx Booking	56
How Smart Scheduler Works	57
Deploying Collaboration Meeting Rooms	57
What are Collaboration Meeting Rooms?	57
Room Size and Quality	57
PIN Protection	57
How Collaboration Meeting Rooms Are Created	57
Differences from TelePresence Conductor-created Conferences	58
Collaboration Meeting Room Resource Consumption	58
Setting up Collaboration Meeting Room	58
Before You Start	58
Connecting to TelePresence Conductor	59
Creating Templates	59

Applying Templates to Groups	64
Setting up Host and Guest Roles in CMRs	64
Host Privileges	64
Allowing the Guest Role	65
Disallowing the Guest Role	65
Including WebEx Participants in CMR meetings	65
Before you start	65
Enabling WebEx in CMRs	66
Making Changes that Affect Collaboration Meeting Rooms	66
Modifying or Replacing the Template for a Group	66
Deleting Templates	67
Deleting Users	67
Moving Users Between Groups	67
Touch Tones and DTMF	67
Auto-connected Participants	68
Add a Favorite Auto-connected Participant	68
Modify a Favorite Auto-connected Participant	68
Deploying FindMe	69
FindMe Basics	69
Deploying FindMe Without Provisioning	69
Defining Caller ID Patterns	69
Assigning a Caller ID Pattern to Imported Accounts	69
Enabling FindMe in Cisco TMSPE	70
Manually Adding FindMe Accounts and Groups	71
Setting up FindMe Locations and Devices	72
Suggested Minimum Setup	72
Adding FindMe Device Templates	72
Adding FindMe location templates	74
Associating Device Templates with Location Templates	74
Assigning Location Templates to Groups	76
Setting up FindMe on Cisco VCS	77
Check FindMe Option Key	77
Set up a Cluster Name	77
Enable and Configure FindMe Settings	77
Sending and Returning Calls via ISDN Gateways	78
Using FindMe to Convert E.164 Alias's to FindMe IDs	78

Using ENUM to Convert E.164 Alias's to FindMe IDs	78
Including the ISDN Gateway Prefix in the Caller ID	79
Regenerating FindMe Locations and Devices	79
Accounts and Groups	80
Location Templates	80
Device Templates	80
Modifying a User's FindMe Locations and Devices	80
Additional Information	81
Determining How to Overwrite a Caller ID with a FindMe ID	81
FindMe in a Cisco VCS Cluster	81
FindMe Accounts Hosted on Hifferent Cisco VCSs in a Network	82
FindMe and Presence	82
Individual and Group FindMe Types	82
Characters Allowed in SIP URIs	82
FindMe Limitations	83
Microsoft Lync Device IDs as FindMe Devices	83
Phone Numbers from Active Directory (AD)	83
Maintaining Users and Devices	84
Synchronizing User Data	84
Mapping of LDAP and AD Fields	84
Testing a Manual Synchronization	84
Running a Manual Synchronization	85
Moving Users and Groups	85
Moving User Accounts Imported from External Sources	85
Moving Groups Between Clusters	85
Searching for User Accounts	85
Renaming Groups and User Accounts	86
Upgrading Software on Provisioned Devices	86
Upgrading Configurations	86
Upgrading Devices	87
Updating Cisco TMS Connection Details	88
Maintaining the Databases	88
Backing up the Databases	88
Restoring the Databases from Backup	88
Moving or Renaming the Databases	88
Troubleshooting	90

Running Cisco TMSPE Diagnostics	90
Running a health check	90
Viewing system status	90
Viewing Cisco VCS Communication History	91
Restarting the TMS Provisioning Extension Windows Service	91
Logs	91
Cisco TMSPE and Cisco TMS Logs	91
Cisco VCS Logs	92
Endpoint Logs	92
Troubleshooting the Installation	92
Checking the Installation Log	92
Unable to Establish SQL Connection Through Java Runtime... ..	92
Unable to Find Valid Certification Path to Requested Target	92
Provisioning Problem Scenarios	93
Database Connection Failure	93
Log Excerpts	93
User Import Fails	93
Email Sending Failure	93
Cisco VCS Reports Data Import Failure	94
Users Get "Out of licenses" Message	94
Signing in Fails When No Template Available	95
Warning Displayed When Uploading Configuration Schema	95
No Phone Books Received	95
Update CMR templates to Support Multiparty license	95
Portal Troubleshooting	96
Cannot Access FindMe or Smart Scheduler	96
Using Search History to Diagnose FindMe Issues	96
Uninstalling Cisco TMSPE	96
Using the Installer	96
Using the Control Panel	96
Reusing or Replacing the Existing SQL Database When Reinstalling	96
Removing Provisioning From a Cisco VCS	97
Document revision history	97
Notices	98
Accessibility Notice	98
Obtaining Documentation and Submitting a Service Request	98

Cisco Legal Information	99
Cisco Trademark	99

Introduction

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

- Large-scale provisioning of telepresence users through Cisco TelePresence Video Communication Server (Cisco VCS)/Expressway.
 - Note: VCS will be referred as above. Unless needed as separate VCS or Expressway (especially in option keys section).
- FindMe, a user-configurable, Cisco VCS/Expressway -based telepresence call forwarding feature.
- 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 their personal provisioning settings, FindMe, Collaboration Meeting Room and Smart Scheduler in a common portal.

Note that Smart Scheduler and Collaboration Meeting Room are also available for deployments with Unified CM rather than Cisco VCS. For guidance, see *Cisco TMSPE with Unified CM Deployment Guide*.

This Deployment Guide

This guide covers the deployment and maintenance of Cisco TMSPE 1.13 with Cisco TMS version 15.7 and Cisco VCS.

Although this guide refers to the Cisco VCS product, it also applies to the Cisco Expressway Series.

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.

Title	Link
<i>Cisco TMSPE Release Notes</i>	http://cisco.com
<i>Cisco TelePresence FindMe User Guide</i>	http://cisco.com
<i>Cisco VCS Administrator Guide</i>	http://cisco.com
<i>Cisco TelePresence Video Communication Server Cluster Creation and Maintenance Deployment Guide</i>	http://cisco.com
<i>Cisco TMS Installation and Getting Started Guide</i>	http://cisco.com
<i>Cisco TMS Administrator Guide</i>	http://cisco.com
<i>ENUM dialing on Cisco VCS Deployment Guide</i>	http://cisco.com
<i>How to enable Windows Installer logging</i>	http://support.microsoft.com/kb/223300
<i>Distinguished Names</i>	http://msdn.microsoft.com

Title	Link
<i>Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters (RFC4515)</i>	http://tools.ietf.org/html/rfc4515

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

Glossary

A glossary of TelePresence terms is available at: tp-tools-web01.cisco.com/start/glossary/

Prerequisites and Recommendations

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

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"> ■ < 200 controlled systems ■ < 100 concurrent participants ■ < 50 concurrent ongoing scheduled conferences 	<ul style="list-style-type: none"> ■ < 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. ■ < 1800 concurrent participants ■ < 250 concurrent ongoing scheduled conferences
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"> ■ < 1000 Collaboration Meeting Rooms ■ < 2000 Cisco VCS-provisioned users (Note: Cisco VCS provisioning not supported on BE6000) 	<ul style="list-style-type: none"> ■ < 48,000 Collaboration Meeting Rooms ■ < 100,000 Cisco VCS-provisioned users
Co-residency	All three applications and Microsoft SQL Server may be co-resident.	<ul style="list-style-type: none"> ■ Cisco TMSXE must be on a dedicated server. ■ Cisco TMS and Cisco TMSPE must use an external SQL Server.

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

	Requirement
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"> ■ Cisco TMS 15.7.
SQL Server connection	<ul style="list-style-type: none"> ■ TCP/IP or Named Pipes protocol must be enabled. TCP/IP is the preferred protocol, see below. ■ SQL Server Browser must be running and able to listen to UDP port 1434.
Windows Server	<ul style="list-style-type: none"> ■ Windows Updates must be enabled. Note that the default connection protocol is TCP/IP. If this protocol is used, no hotfixes are required.
Cisco TMS Provisioning Extension option key	<ul style="list-style-type: none"> ■ Must be added in Cisco TMS under Administrative Tools > General Settings, in the Licenses and Option Keys pane. ■ License consumption is based on usage; the number of concurrent signed-in and provisioned devices. A user signed in to several devices simultaneously will consume one license per device.
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 www.java.com.</p> <p>Caution: 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 **tmsg**, 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 VCS requirements

VCS Control must be version X8.10.

In order to use provisioning or FindMe, option keys must be added for:

- Cisco VCS Device Provisioning.
- FindMe, if applicable.

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.

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"> ■ <i>sysadmin</i> if the installer will create the database on the MS SQL server ■ <i>db_owner</i> if using a manually created database on the MS SQL server. See Required security permissions, page 18 for further details.

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 18](#) 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 1.13 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"> ■ Screen licenses on TelePresence Server. ■ Appropriate MCU port licenses. ■ Shared Multiparty License / Personal Multiparty License on Conductor.
Smart Scheduler	None
Option key:	<ul style="list-style-type: none"> ■ Cisco TMS <ul style="list-style-type: none"> - Cisco TMS Provisioning Extension option key ■ VCS Series <ul style="list-style-type: none"> - Device Provisioning key - FindMe ■ Expressway Series <ul style="list-style-type: none"> - Registration licenses - FindMe
FindMe	<p>FindMe option key required on the following:</p> <ul style="list-style-type: none"> ■ Cisco VCS series ■ Cisco Expressway Series <p>FindMe</p>

Best practices for deployment

Upgrade endpoints to the latest software

Prior to installation and deployment of Cisco TMSPE, we recommend upgrading all endpoints being provisioned through Cisco TMSPE device provisioning.

This limits the number of templates and schemas to maintain post-installation.

Supported endpoints

If an endpoint has a published configuration template schema, the endpoint is compatible with Cisco TMSPE.

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.

Make sure the encryption settings match the available certificates when configuring Cisco VCS communication, see [Setting up Communication Between Cisco TMS and Cisco VCS, page 31](#).

Synchronize time in Cisco VCS and Cisco TMS

Keep time synchronized between Cisco TMS and Cisco VCS. We recommend configuring them to use the same NTP (Network Time Protocol) server :

- To configure the NTP server in Cisco VCS, go to **System > Time**.
- Cisco TMS uses the NTP setting for the host Windows Server operating system. For instructions, see the Microsoft support article [How to configure an authoritative time server in Windows Server](#). The time setting on the Windows server must be correct for Cisco TMS to function correctly, and the date and time on the Cisco TMS and SQL Server must be identical, if the servers are separate.

We therefore strongly recommend keeping both servers in the same Active Directory domain and setting them up to use the same NTP (Network Time Protocol) server.

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.

Configuring Cisco VCS for Provisioning

When deploying provisioning for the first time, Cisco VCS must be configured for provisioning prior to installing and activating Cisco TMSPE.

Provisioning Within Your Network

There are two types of Cisco VCS:

- **VCS Control:** this is designed to be installed in the organization's private network to provide registration and routing capabilities to H.323 and SIP based endpoints used within the business or connected into the business over a VPN .
- **VCS Expressway:** this is designed to be installed in the organization's DMZ to provide registration and routing capabilities for public and home based H.323 and SIP based endpoints. The VCS Expressway also provides firewall traversal capabilities to allow communication with the internal VCS Control and endpoints that are registered to it.

In a network which only has VCS Expressways, you can configure your system with provisioning enabled on the VCS Expressway, however, you should consider the security aspects of storing user data on an appliance that is located in a DMZ.

User accounts can only reside on one Cisco VCS (or Cisco VCS cluster). Therefore if your network has a combination of VCS Expressways and VCS Controls (where some endpoints - such as soft clients - may register to either the VCS Control or the VCS Expressway), we recommend that you configure and enable provisioning only on the VCS Control (or VCS Control cluster). If a soft client or other endpoint registers to a VCS Expressway, provisioning requests will be routed (using search rules) to the VCS Control associated with the VCS Expressway via the appropriate traversal zone.

In hierarchical Cisco VCS deployments you could use one or more dedicated Cisco VCS clusters for provisioning—all other Cisco VCSs could be configured to route provisioning requests to those dedicated provisioning servers. However, each provisioning Cisco VCS cluster is still subject to the 10,000 user capacity limits that would apply to a any Cisco VCS cluster. If you need to provision more than 10,000 users, your network will require additional Cisco VCS clusters with an appropriately designed and configured dial plan.

If provisioning is enabled on any VCS Control or VCS Expressway that does not need to have provisioning enabled, be sure to disable it by using the process specified in [Removing Provisioning From a Cisco VCS, page 97](#).

Setting up DNS for the Cisco VCS

Cisco VCS must use DNS and be addressable via DNS. To configure the Cisco VCS's DNS server and DNS settings:

1. Go to **System > DNS**.
2. Set **System host name** to be the DNS hostname for this Cisco VCS (typically the same as the **System name** in **System > Administration**, but excluding spaces).
3. Set **Domain name** so that **<System host name>. <Domain name>** is the unique FQDN for this Cisco VCS.
4. In the **Default DNS servers** section, set **Address 1** to the IP address of a DNS server for Cisco VCS to use.
5. Click **Save**.

Installing the Device Provisioning Option Key

Provisioning is activated by installing the Device Provisioning option key on the Cisco VCS. Contact your Cisco representative for more information about how to obtain the Device Provisioning option key.

If the Cisco VCS is in a cluster, option keys must be set manually on each Cisco VCS, and must be identical (except for the call license keys) on all Cisco VCSs in the cluster.

To add the option key:

1. On the Cisco VCS, go to **Maintenance > Option keys**.
2. To make sure the key isn't already installed, check the list of existing option keys on the upper part of the screen. The **System information** section tells you the hardware serial number and summarizes the installed options.
3. Under **Software option**, enter the 20-character option key that has been provided to you for the option you want to add.
4. Click **Add option**.

The screenshot displays the 'Option keys' page in the Cisco VCS interface. At the top, there are navigation tabs: Status, System, Configuration, Applications, Users, and Maintenance. The 'Option keys' section contains a table with the following data:

Key	Description
<input type="checkbox"/> 110341120-1-0710001	Microsoft Interoperability
<input type="checkbox"/> 110341120-1-0710002	H323-SIP Interworking Gateway
<input type="checkbox"/> 110341120-1-0710003	Dual Network Interfaces
<input type="checkbox"/> 110341120-1-1172000	Expressway
<input type="checkbox"/> 110341120-1-0710004	FindMe
<input type="checkbox"/> 110341120-1-0010010	50 Traversal Calls
<input type="checkbox"/> 110341120-1-0000012	25 Non-traversal Calls

Below the table are buttons for 'Delete', 'Select all', and 'Unselect all'. The 'System information' section shows the hardware serial number as '0240211' and active options as '25 Non Traversal Calls, 50 Traversal Calls, 2500 Registrations, 0 TURN Relays, Expressway, Encryption, Interworking, FindMe, Dual Network Interfaces, Enhanced OCS Collaboration'. The 'Software option' section has a text input field for 'Add option key' with a red asterisk and a help icon. At the bottom is an 'Add option' button.

Enabling SIP

SIP must be enabled on each VCS Control and VCS Expressway in the network:

1. Ensure that **SIP mode** is turned on (**Configuration > Protocols > SIP**). This is enabled by default.
2. Ensure that at least one SIP domain is specified (**Configuration > Domains**).

Configuring How Cisco VCS Handles Calls to Unknown IP Addresses

The **Calls to unknown IP addresses** setting determines the way in which the Cisco VCS attempts to call systems which are not registered with it or one of its neighbors.

It is configured on the **Dial plan configuration** page (**Configuration > Dial plan > Configuration**).

VCS Control

On the VCS Control, set **Calls to unknown IP addresses** to *Indirect*.

The screenshot shows the Cisco TelePresence Video Communication Server Control interface. The top navigation bar includes Status, System, Configuration, Applications, Users, and Maintenance. The current page is 'Dial plan configuration'. The configuration area has two fields: 'Calls to unknown IP addresses' set to 'Indirect' and 'Fallback alias' which is empty. A 'Save' button is located below the configuration area.

VCS Expressway

If you are using a VCS Expressway, **Calls to unknown IP addresses** must be set to *Direct*.

The screenshot shows the Cisco TelePresence Video Communication Server Expressway interface. The top navigation bar includes Status, System, Configuration, Applications, Users, and Maintenance. The current page is 'Dial plan configuration'. The configuration area has two fields: 'Calls to unknown IP addresses' set to 'Direct' and 'Fallback alias' which is empty. A 'Save' button is located below the configuration area.

Adding Cisco VCS to Cisco TMS

This procedure is compulsory for the Cisco VCS (or Cisco VCS cluster) on which provisioning is enabled (typically the VCS Control), and optional for other Cisco VCSs (a VCS Expressway, for example).

In each Cisco VCS:

1. We recommend enabling SNMP as this is the best way for Cisco TMS to be able to detect and add the Cisco VCS:
 - Go to **System > SNMP** and ensure that **SNMP mode** is set to *v3 plus TMS support* and that a **Community name** is set.
 - If SNMP is not permitted inside your network, you can add VCS Control to Cisco TMS without SNMP. However, this will negatively impact Cisco TMS's ability to auto-discover and monitor the Cisco VCS.
2. Ensure that the **Address** (IP address or FQDN) of Cisco TMS is set up in **System > External manager**.

The screenshot shows the Cisco TMS configuration page for 'External manager'. The top navigation bar includes Status, System, Configuration, Applications, Users, and Maintenance. The current page is 'External manager'. The configuration area has four fields: 'Address' set to '10.44.9.141', 'Path' set to 'tms/public/external/management/SystemManagementService.asmx', 'Protocol' set to 'HTTP', and 'Certificate verification mode' set to 'On'. A 'Save' button is located below the configuration area.

In Cisco TMS, add the Cisco VCS:

1. In Cisco TMS, go to **Systems > Navigator**.
2. In the left pane, select the folder where you want to add the Cisco VCS.
3. Click the **Add by Address** button in the right pane. Follow the instructions in Cisco TMS to add the Cisco VCS.

4. Enter the FQDN of the Cisco VCS, for example `vcs1.example.com`, and click **Next**. Cisco TMS will collect information from the VCS about how best to communicate with it.

Enabling Provisioning on the Cisco VCS

Setting up a Cisco VCS cluster and enabling provisioning are separate processes and should not be attempted simultaneously. If you want to set up a Cisco VCS cluster, first set up the cluster name and complete the provisioning configuration as described below. Then set up the cluster as described in [Cisco VCS Cluster Creation and Maintenance Deployment Guide](#).

Setting up a Cluster Name

You must set up the Cisco VCS with a cluster name regardless of whether it is part of a cluster. The cluster name must be unique compared to any other Cisco VCS or Cisco VCS cluster managed by this Cisco TMS

To set up or change the cluster name:

1. Go to **System > Clustering**.
2. Enter the **Cluster name**:
 - If the Cisco VCS is part of a cluster, set it to the fully qualified domain name used in SRV records that address the cluster, for example "cluster1.example.com".
 - If the Cisco VCS is not part of a cluster, set it to the fully qualified domain name used in SRV records that address the Cisco VCS, for example "vcs1.example.com".
3. Click **Save**.

Enabling Presence on the Cisco VCS

Endpoints such as Jabber Video can use Cisco VCS as a presence server to share presence information (for example *Offline*, *Online*, *Away*, or *Busy*) with other users.

- You must only enable presence on a single Cisco VCS or Cisco VCS cluster per SIP domain in your deployment.
- Enabling Presence is optional.

Presence on VCS Control

1. In VCS Control, go to **Applications > Presence** and set **SIP SIMPLE Presence Server** to *On*.
2. If VCS Control is to publish presence on behalf of endpoints registered to it that do not publish their own presence (that is, endpoints other than Jabber Video), you must also set **SIP SIMPLE Presence User Agent** to *On*.

The screenshot shows the Cisco TelePresence Video Communication Server Control web interface. The navigation menu includes Status, System, Configuration, Applications, Users, and Maintenance. The current page is 'Presence' under the 'Applications' section. The 'Presence' section is divided into two main areas: 'PUA' and 'Presence Server'. In the 'PUA' section, 'SIP SIMPLE Presence User Agent' is set to 'On' and 'Default published status for registered endpoints' is set to 'Online'. In the 'Presence Server' section, 'SIP SIMPLE Presence Server' is set to 'On'. A 'Save' button is located below the configuration fields. At the bottom, a 'Status' table shows the following:

Status	
Presence User Agent	Active
Presence Server	Active

Presence on VCS Expressway

1. In VCS Expressway, go to **Applications > Presence** set **SIP SIMPLE Presence Server** to *Off*.
The Presence Server must not be enabled on VCS Expressway; VCS Expressway must pass presence information to the Presence Server on VCS Control rather than keep the presence information locally.
2. If VCS Expressway is to publish presence on behalf of endpoints registered to it that do not publish their own presence (that is, endpoints other than Jabber Video), you must set **SIP SIMPLE Presence User Agent** to *On*.

The screenshot shows the Cisco TelePresence Video Communication Server Expressway web interface. The navigation menu includes Status, System, Configuration, Applications, Users, and Maintenance. The current page is 'Presence' under the 'Applications' section. The 'Presence' section is divided into two main areas: 'PUA' and 'Presence Server'. In the 'PUA' section, 'SIP SIMPLE Presence User Agent' is set to 'On' and 'Default published status for registered endpoints' is set to 'Online'. In the 'Presence Server' section, 'SIP SIMPLE Presence Server' is set to 'Off'. A 'Save' button is located below the configuration fields. At the bottom, a 'Status' table shows the following:

Status	
Presence User Agent	Active
Presence Server	Inactive

Verifying Device Authentication

The Cisco VCS's Provisioning Server requires that any provisioning or phone book requests it receives have already been authenticated at the zone or subzone point of entry into the Cisco VCS. The Provisioning Server does not do its own authentication challenge and will reject any unauthenticated messages.

Verify that each of the zones and subzones listed below are configured with an **Authentication policy** of either *Check credentials* or *Treat as authenticated*.

- The Default Zone (**Configuration > Zones > Zones** and select the **Default Zone**)
- Any traversal client zones (**Configuration > Zones > Zones**, then select each zone of type *Traversal client*)
- The Default Subzone (**Configuration > Local Zone > Default Subzone**)
- Any other configured subzones (**Configuration > Local Zone > Subzones**, then select each subzone to verify their configurations)

For more information about setting up device authentication, see [Device Authentication on Cisco VCS Deployment Guide](#).

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 30](#).
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 30](#).

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 1.13

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 'Provisioning Mode' dropdown menu is highlighted, showing three options: 'Off', 'Provisioning Extension', and 'Provisioning Extension'. The 'Provisioning Extension' option is selected. Other settings visible include TMS Release Key, Default ISDN Zone, Default IP Zone, Default User Language, Software FTP Directory, System Contact Name, System Contact E-mail Address, Global Phone Book Sort, Route Phone Book Entries, Cisco System Phone Books, Phone Books Update Frequency, Phone Books Update Time of Day, Alternate System Name Rules for Endpoints and Rooms, Enable Auditing, Enable Login Banner, Show Systems In Navigator Tree, and Enable TMS Redundancy.

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 92](#).
 - **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 92](#) for further information.
4. When browsing to all of the above Cisco TMSPE pages is successful and no alarms are reported in **Provisioning Extension Diagnostics**, proceed to [Setting up Communication Between Cisco TMS and Cisco VCS, page 31](#).

Setting up Communication Between Cisco TMS and Cisco VCS

Perform this procedure to enable the Cisco VCS or VCS clusters to communicate with Cisco TMSPE. If Cisco VCSs are clustered, configure only one Cisco VCS in the cluster.

- Cisco VCS imports the user configurations, FindMe settings, phone books and licensing information from Cisco TMSPE.
- Cisco TMSPE receives information about provisioned devices from Cisco VCS.

Follow these steps:

1. In Cisco TMS, go to **Systems > Navigator** and select the Cisco VCS. This can be any Cisco VCS from the cluster.
2. Click the **Provisioning** tab.
3. At the bottom of the page, click the **Set Default Connection Settings** button.
The **Cisco TMS Connection Settings** pane is populated with suggested values.

4. Adjust the connection settings according to your telepresence infrastructure.

The screenshot shows a 'Configuration' window with a 'TMS Connection Settings' section. The settings are as follows:

Server Address:	10.47.28.205
Encryption:	Off
Certificate Verification Enabled:	No
Certificate Hostname Checking Enabled:	No
Username:	administrator
Password:
Base Group:	Unknown (0a3a0732-7d24-4833-ab4d-26d63f06d062)

- The default and recommended **Encryption** setting is *TLS*, see [Use secure communication, page 22](#). If opting not to use secure communication, make sure to change this setting to *Off*, or the connection will be refused. If enabling encryption, also select whether to check for a valid certificate and certificate hostname.
 - The username and password must be for a member of the Site Administrators group in Cisco TMS.
 - In a large deployment, make sure **Base Group** is set on a group level per Cisco VCS cluster, not at the root level.
5. Scroll down to the **Services** pane and check **Enable Service** for each of the services listed, including FindMe if applicable.
6. Click **Save**.
7. Check the **Status** field for each of the enabled services. If errors are displayed for any of the services, click the corresponding warning icon and follow the instructions displayed. Then click **Force Refresh**.

The screenshot shows the 'Services' pane with the following configurations:

Service	Enable Service	Polling Interval	Status
Users	<input checked="" type="checkbox"/>	2 minutes	OK (click for details)
FindMe	<input checked="" type="checkbox"/>	2 minutes	OK (click for details)
Phone Books	<input checked="" type="checkbox"/>	3 hours	OK (click for details)
Devices	<input checked="" type="checkbox"/>	Base Group: root	OK (click for details)

At the bottom of the Services pane, there are buttons for: Save, Force Refresh, Set Default Connection Settings, Check for Updates, and Perform full Synchronization.

8. When green check marks are displayed for all services, click **Save**.

You can now proceed to [Setting up Users and Provisioning, page 35](#).

Table 1 Settings on the Provisioning tab

Field and buttons	Description
Save	Save the settings
Force Refresh	Sends the current settings available in Cisco VCS page, as the same settings on the Cisco VCS UI must be same as seen in Cisco TMS.
Set Default Connection Settings	Set default connection settings.
Check for Updates	Triggers Cisco VCS to search for the changes in the data-set from the last time that Cisco VCS checked for changes in it.
Perform full Synchronization	Use in special cases when groups are moved or databases are restored. This creates inconsistencies in the datasets on the Cisco VCS and Cisco TMSPE.

Setting up Users and Provisioning

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 eliminates scalability with Cisco VCS clusters and complicates bulk deletion of users.

Setting up Groups

We recommend that you group users according to their geographical location to match the organization of your organization's Cisco VCSs. Each group must not exceed 10 000 users, as this is the maximum number of users allowed by Cisco VCS.

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 20](#).
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: fqdn.example.com

Port: 3268

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
Hostname	Yes	Yes	Yes	Server hosting the external directory. Provide a fully qualified domain name (FQDN).
Port	Yes	Yes	Yes	Port on the server used for accessing the external directory. Use Global Catalog port 3268 for Kerberos import.
Username	Yes	Yes	Yes	User name Cisco TMSPE uses when logging on to the external directory. See also Password.
Password	Yes	Yes	Yes	Password Cisco TMSPE uses when logging on to the external directory. See also Username.
Base dn	Yes	Yes	Yes	LDAP distinguished name. See the MSDN Library article Distinguished Names for more information.
Relative search dn	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 Distinguished Names .
Search filter	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: Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters .
Distribution center	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.
Distribution center timeout	No	Yes	No	Maximum number of milliseconds to wait for a reply from the Key Distribution Center.
Realm	No	Yes	No	Realm configured in AD for Kerberos Authentication.
Connection type	No	No	Yes	Select the connection type. The available options are: <ul style="list-style-type: none"> – <i>Unsecured</i> – <i>StartTLS</i> – <i>SSL</i>– note that no certificate handling is supported for this connection type.

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 84](#).

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.

To change Active Directory 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.

To change LDAP field mapping for new user imports:

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 * (milliseconds)

Filter Template *

Follow Referrals * Yes No

 Save  Cancel  Restore Default

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 39](#).

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**.

Creating Address Patterns

Address Pattern Types

Cisco TMSPE has two main types of address patterns:

- Device address patterns are templates that Cisco TMSPE uses to create addresses for provisioned devices. You must assign device address patterns so that Cisco TMSPE can connect users to their devices.
- Video address patterns are used for generating the video addresses that serve both as FindMe IDs (if FindMe is used) and as the main addresses for users in the provisioning phone book source. The video address can be a SIP URI, an H.323 ID, or an E.164 Alias.

Note: User must have a video address configured to appear in a provisioned users phonebook. Users without a video address may appear in the Phone Book Source contact list, but will not appear in the Phone Book contact list.

Additionally:

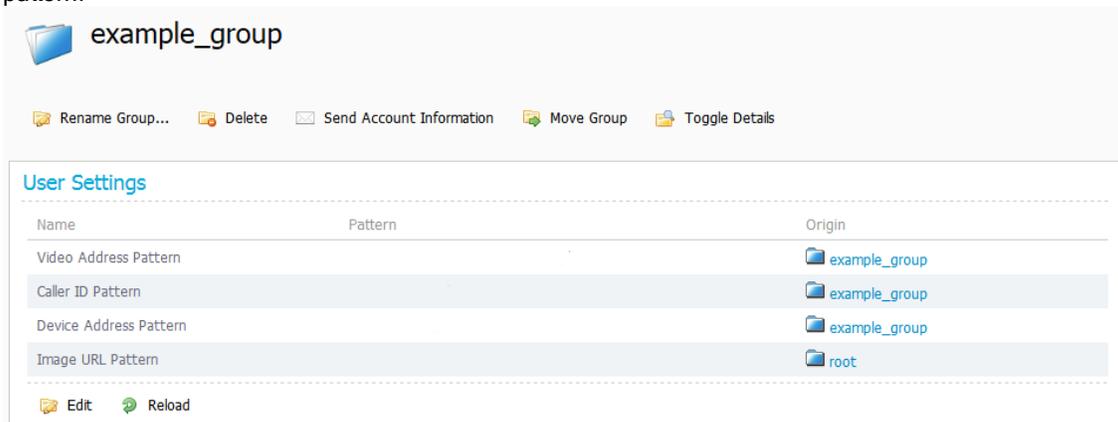
- The **Caller ID pattern** is used by FindMe to generate caller IDs for calls routed through an ISDN gateway. [Defining Caller ID Patterns, page 69](#) is described in the [Deploying FindMe, page 69](#) section of this document.
- An **Image URL pattern** may optionally be added when configuring user groups, if a server with user images is available. The images will be used by the Cisco TMSPE and FindMe user interfaces and in phone books on compatible devices.

Note that any pattern assigned to a group is inherited by all users in the group, all subgroups, and all users in subgroups.

Adding the Patterns

To create a device address pattern, a video address pattern, and optionally an image url pattern:

1. In Cisco TMS, go to **Systems > Provisioning > Users**.
2. In the **Users and Groups** container, navigate to and click the group to which you want to assign a device address pattern.



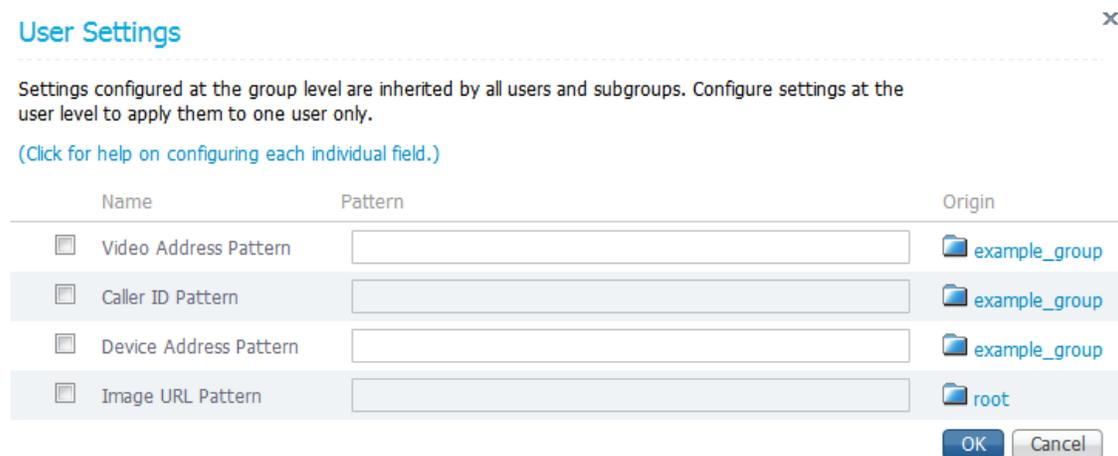
example_group

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

Name	Pattern	Origin
Video Address Pattern		example_group
Caller ID Pattern		example_group
Device Address Pattern		example_group
Image URL Pattern		root

Edit Reload

3. In the **User Settings** pane, click **Edit**. The **User Settings** dialog box opens.



User Settings

Settings configured at the group level are inherited by all users and subgroups. Configure settings at the user level to apply them to one user only.

(Click for help on configuring each individual field.)

Name	Pattern	Origin
<input type="checkbox"/> Video Address Pattern	<input type="text"/>	example_group
<input type="checkbox"/> Caller ID Pattern	<input type="text"/>	example_group
<input type="checkbox"/> Device Address Pattern	<input type="text"/>	example_group
<input type="checkbox"/> Image URL Pattern	<input type="text"/>	root

OK Cancel

4. In the **Video Address Pattern** field, specify the pattern that you want Cisco TMSPE to use when defining FindMe IDs for users in the selected group, or the explicit FindMe ID for the selected user. You can use any of the following user attributes in the pattern:

- {username}
- {display_name}
- {first_name}
- {last_name}
- {email}
- {office_phone}
- {mobile_phone}

5. In the **Device Address Pattern** field, specify the pattern that you want Cisco TMSPE to use when creating names of provisioned devices.

You can use any of the above listed user attributes in the pattern. You can also use any of the following device attributes in the pattern:

- {device.model}
This resolves to the device model; for example, e20, movi, ex90.
- {device.connectivity}
This resolves to *internal* if the device is registered to a VCS Control, or *external* if registered to a VCS Expressway.

User Settings ✕

Settings configured at the group level are inherited by all users and subgroups. Configure settings at the user level to apply them to one user only.

[\(Click for help on configuring each individual field.\)](#)

Name	Pattern	Origin
<input checked="" type="checkbox"/> Video Address Pattern	<input type="text" value="{first_name}.{last_name}@example.com"/>	 example_group
<input type="checkbox"/> Caller ID Pattern	<input type="text"/>	 example_group
<input checked="" type="checkbox"/> Device Address Pattern	<input type="text" value="{username}.{device.model}@example.com"/>	 example_group
<input type="checkbox"/> Image URL Pattern	<input type="text"/>	 root

6. Optionally, in the Image URL Pattern field, specify the pattern to use when collecting images of the users. Supported formats are **.jpg**, **.jpeg**, and **.png**. You can use any of the following user attributes in the pattern:

- {username}
- {display_name}
- {first_name}
- {last_name}
- {email}
- {office_phone}
- {mobile_phone}

7. Click **OK**.

Example Patterns

Video Address

- {username}@example.com
- {email}

Device Address

- {username}.{device.model}@example.com
- {username}.{device.model}.{device.connectivity}@example.com

Advanced Parameters (Regex)

When working with user setting (**Video Address Pattern**, **Caller ID Pattern**, **Device Address Pattern**) and when edit or creating CMR templates (**SIP Alias Pattern**) you have the option to use regex to remove or change the value of these field. All these fields uses fields from AD/LDAP.

You can use as many regex replacements as you need.

Example of simple format:

```
{<name_of_ldap_field>}
```

Example of simple regex replacement:

```
{<name_of_ldap_field>[<regex>='<replacement_value>']}
```

The following examples show how you can use regex substitutions in the pattern:

- `{username [' '=']} . {device.model}@example.com`
This substitution removes spaces from the pattern.
- `{username} . {device.model} . {device.connectivity['internal'='office', 'external'='home']}@example.com`
This substitution changes the connectivity from 'internal' to 'office' and from 'external' to 'home'.
- `{username} ['^\\w' '= ']@example.com`
This example strips all character except the letters a-z. It is possible to also use numbers and underscore.

Image URL

```
http://yourimageserver/users/{username}.png
```

Setting up Configurations for Provisioned Devices

To provision devices with a desired set of configurations, you must create templates in Cisco TMSPE and assign them to groups of users. Each template must be based on a valid schema; an XML file containing all the possible configurations supported by a specific model and version of a device.

To set up configurations, you must obtain and upload template schemas for each type of endpoint used in your deployment, before you can add configuration templates and assign them to groups.

Obtaining Template Schemas

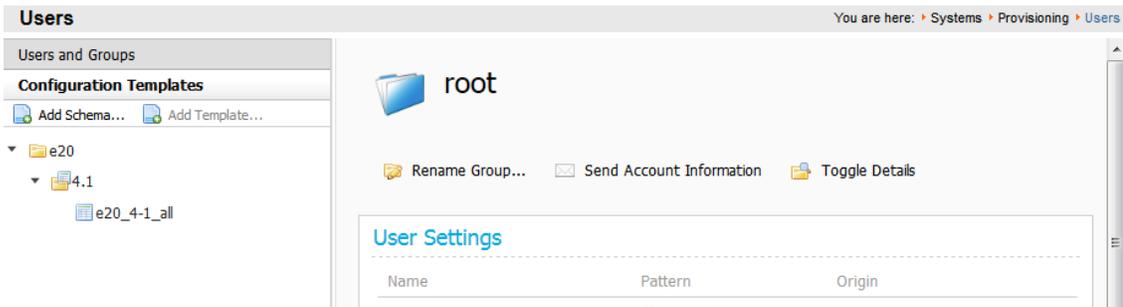
For each model and version of endpoints available on your network, you must obtain the relevant schema and upload it to Cisco TMSPE. Template schemas are usually included with device software releases, either inside the software bundle, or on the same page as the release notes are made available. If the schema is not included with the software bundle, use the search facility on <http://cisco.com> to locate the template schema, and then download it to your local server:

To download a compatible template schema and add it to Cisco TMSPE:

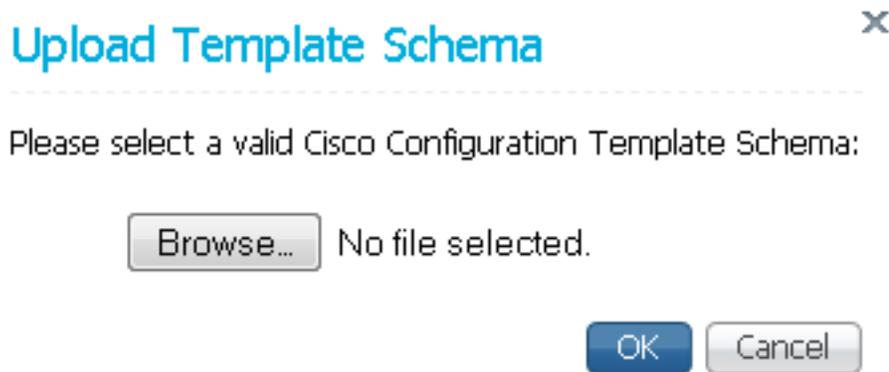
1. Enter "Configuration Templates for TMS" (including the quotation marks) as your search string.
2. Scroll down the list of search results to locate the .zip file containing the required schema.

Uploading the Schema to Cisco TMS

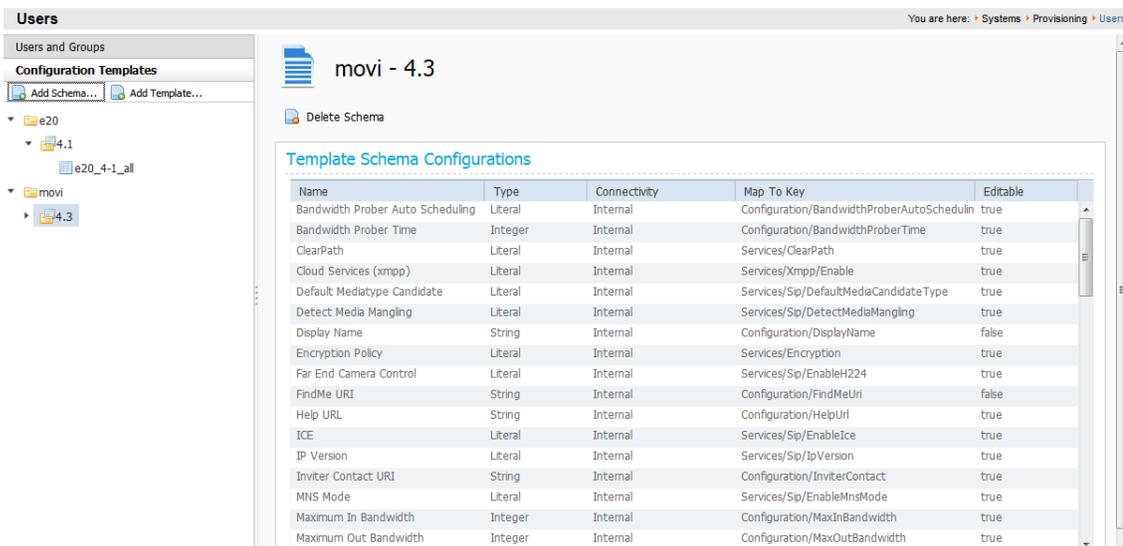
1. In Cisco TMS, go to **Systems > Provisioning > Users**.
2. On the **Users** page, click the **Configuration Templates** container. Folders are displayed representing models and versions of devices for which template schemas have already been uploaded.



3. In the **Configuration Templates** container, click **Add schema**. The **Upload Template Schema** dialog box opens.



4. Click the **Browse** button, navigate to the folder on your local server to where you downloaded the schema, select it, and then click **OK**. The template schema is added in the relevant folder for the relevant model and version of device.



Adding Configuration Templates

A configuration template specifies the collection of configurations that you choose to assign to groups of users. The configurations that you choose from are defined in the associated template schema (see [Obtaining Template Schemas, page 42](#)).

Depending on the types of endpoint devices on your network and the services in use, the following configurations are usually the most important:

- **SIP server address**
- **Phonebook URI**
- **Presence URI**

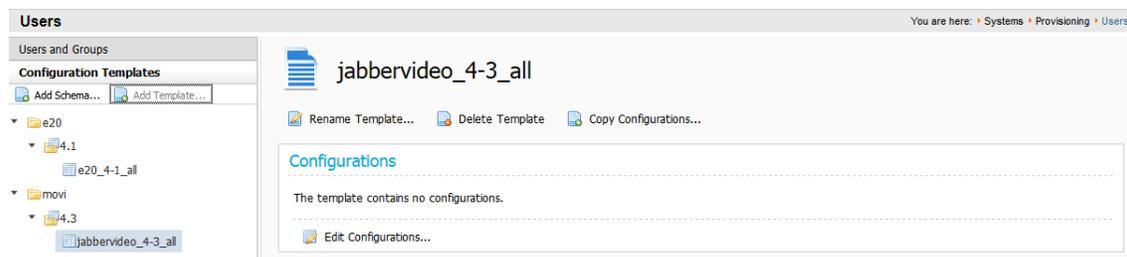
For details on the available configurations and restricted values for each type of endpoint, see the administrator documentation for the endpoint.

To create a configuration template:

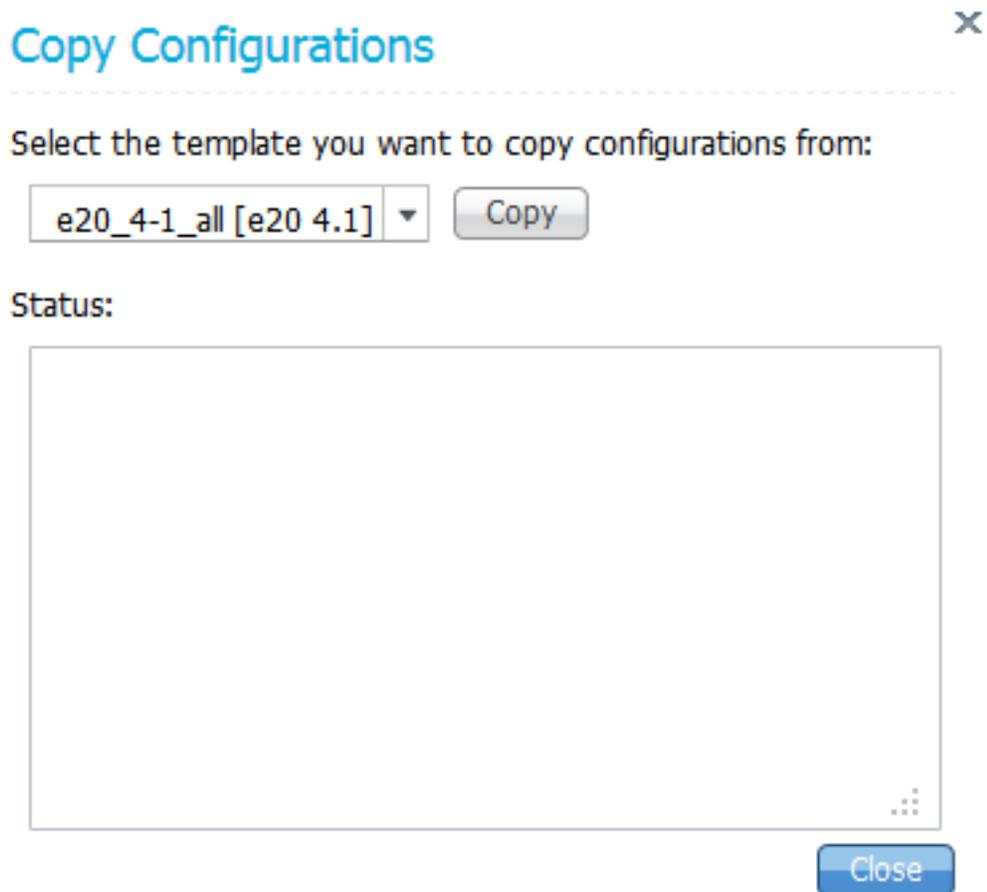
1. On the **Users** page, click the **Configuration Templates** container.
2. In the **Configuration Templates** container, navigate to the folder for the relevant model and version of device, and then click **Add template**. The **Add Template** dialog box opens.



3. Enter a suitable display name for the template, and then click **OK**. The template is added to the **Configuration Templates** container. At this point, the template contains no configurations.



4. Add configurations in either of the following ways:
 - Copy configurations from an existing template:
 1. Above the **Configurations** pane, click **Copy Configurations**. The **Copy Configurations** dialog box opens.



2. Select the template from which you want to copy all configurations, and then click **Copy**. The **Status** field reports the result of the copy. The number of successfully copied configurations is displayed, as well as the number that failed to copy, for example, due to the target template's schema not supporting the same keys as the originating template's schema.

Copy Configurations ✕

Select the template you want to copy configurations from:

Status:

1 of 2 configurations were successfully copied

1 failures:

1 : ConfigurationProvisioningMode is not supported by this template's schema

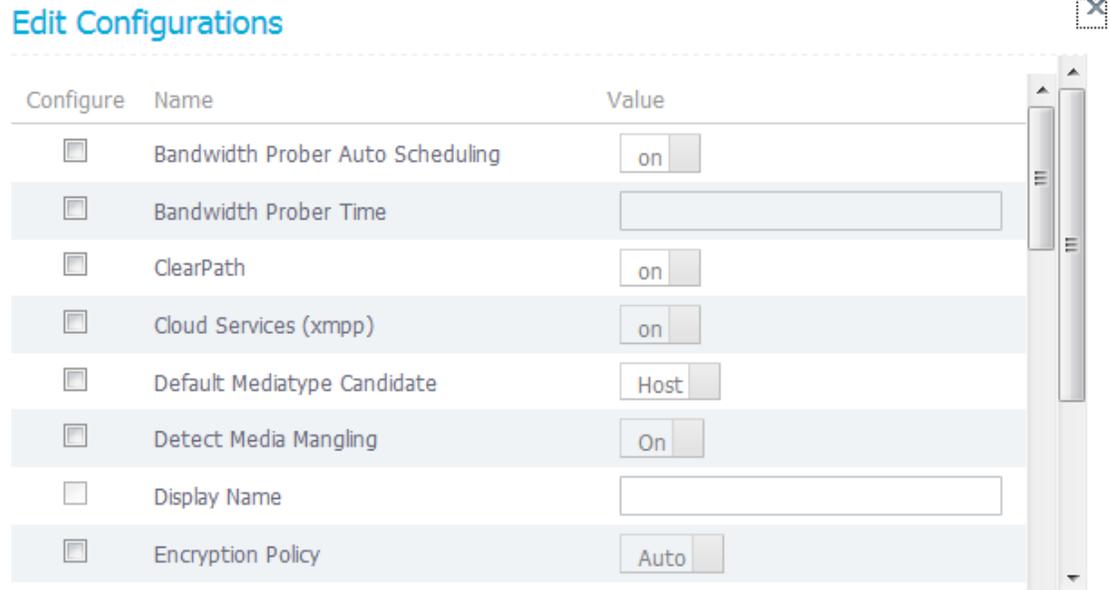


Close

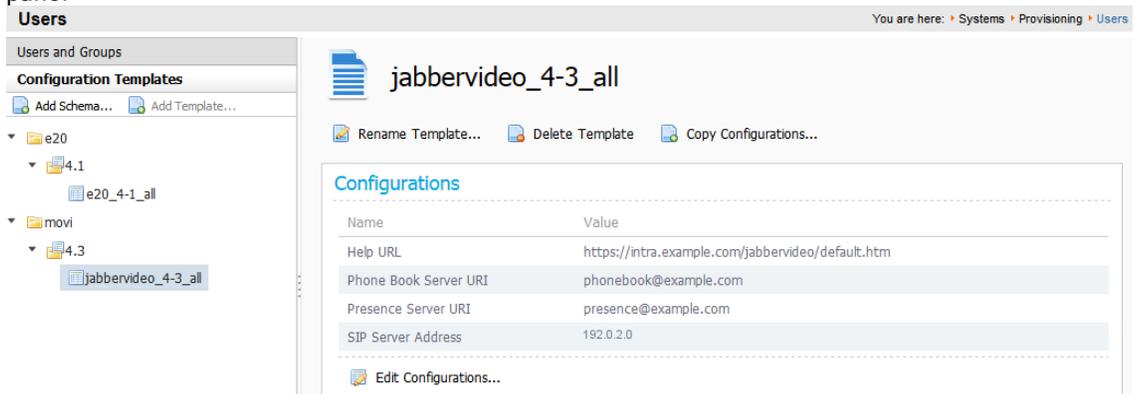
3. Click **Close**.

– Add individual configurations:

1. In the **Configurations** pane, click **Edit configurations**. The **Edit Configurations** dialog box opens.



2. Select the **Configure** check box for each configuration that you want to add to the template, and then select or enter a value in the **Value** field.
3. Click **Save** to save your settings. The configurations you have added are displayed in the **Configurations** pane.



You can now assign the configuration template to one or more groups of users.

Assigning Configuration Templates to Groups

Any configuration template you assign to a group is inherited by all users in the group, all subgroups, and all users in subgroups. You cannot assign a configuration template directly to an individual user. If multiple configuration templates exist for a particular model and version, you cannot assign more than one of them to a group.

To assign a configuration template to a group:

1. On the **Users** page, click the **Users and Groups** container, and then click the required group. Scroll down to the **Configuration Templates** pane.

Configuration Templates

Name	Model	Version	Origin
e20_4-1_all	e20	4.1	root

 Assign Templates

- Click **Assign templates**. The **Assign Templates** dialog box opens.

Assign Templates

Assign	Name	Model	Version	Origin
<input type="checkbox"/>	e20_4-1_all	e20	4.1	root
<input type="checkbox"/>	jabbervideo_4-3_all	movi	4.3	

Save

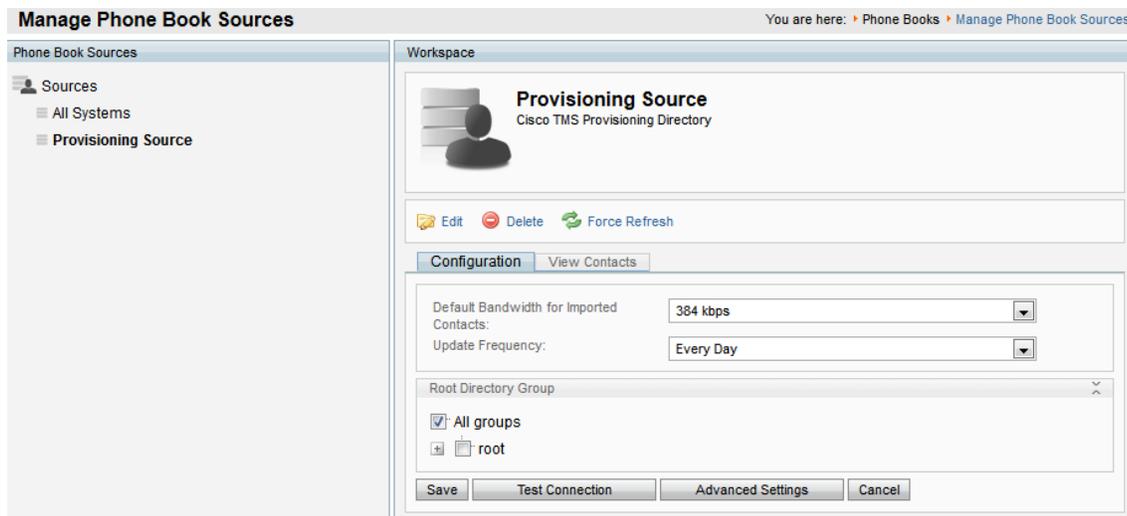
Cancel

- Select the check box for each configuration template that you want to assign to the group.
- Click **Save**.

Provisioning Phone Books

You do not set phone books to provisioned endpoints the same way as with Cisco TMS-registered endpoints. The **Phone Book URI** you configure for groups, for example `phonebook@example.com`, is used to provision users with one or more phone books that they have been given access to.

Creating and Configuring Provisioning Phone Book Sources



Manage Phone Book Sources You are here: Phone Books > Manage Phone Book Sources

Phone Book Sources

- Sources
 - All Systems
 - Provisioning Source

Workspace

Provisioning Source
Cisco TMS Provisioning Directory

Edit Delete Force Refresh

Configuration View Contacts

Default Bandwidth for Imported Contacts: 384 kbps

Update Frequency: Every Day

Root Directory Group

- All groups
- root

Save Test Connection Advanced Settings Cancel

You can create one provisioning source from the root folder of the user directory, or multiple provisioning sources with different root directories, so that you can give groups access to more limited phone books.

For more information about how phone books and sources work, see [Cisco TelePresence Management Suite Administrator Guide](#) or the built-in web help.

To create a provisioning source:

1. In Cisco TMS, go to **Phone Books > Manage Phone Book Sources**.
2. In the right-hand pane, click **New**.
3. In the **Name** field, add a descriptive name for the new source.
4. From the **Type** drop-down menu, select *Cisco TMS Provisioning Directory*.
5. Click **Save**.

Follow procedure below to modify the configuration of the new provisioning source, including its root directory.

To modify the configuration of an existing provisioning source:

1. Go to **Phone Books > Manage Phone Book Sources** and select the provisioning source in the left-hand pane.
2. Click the **Advanced Settings** button to open settings that configure what is included in the source .
 - Check **Import Provisioned Devices** to have device addresses added to the source as users log in and devices are provisioned.
 - Check **Import Office Phone** and **Import Mobile Phone** to include these fields for imported or manually created provisioning users.
3. In the **Root Directory Group** pane, check the group you want to base this provisioning source on.
4. Click **Save**.

Creating Additional Provisioning Phone Books

In order to be used as phone books, you must connect your provisioning sources to new or existing phone books in Cisco TMS.

To create a new phone book:

1. Go to **Phone Books > Manage Phone Books**.
2. Click **New**.
3. Enter a display name for the phone book and click **Save**.

To connect one or more provisioning sources to an existing phone book:

1. Go to **Phone Books > Manage Phone Books**.
2. In the left-hand pane, click on the desired phone book.
3. In the right-hand pane, click the **Connect** button.
4. Check the provisioning source or sources you want to connect.
5. Click **OK**.

Phone Book Sources Activity Status

Monitor the activity status by going to **Phone Books > Phone Book Sources Activity Status** in Cisco TMS.

Phone Book Sources Activity Status You are here: Phone Books > Phone Book Sources Activity Status

Information

Get an overview of activity status on events. See which events has been run and if they failed or succeeded. Click on "View" link on the right to see more detailed log.

Start Date: 3/29/2012 End Date: 3/29/2012 Show only mine Search

Start Time	Scheduled by	Description	Progress	Recurrence	Status
3/29/2012 10:08:47 AM	User, System	Phone Book Source update All Systems	100% Event successful	Every 5th minute	Success

1 Records per Page 20 Displaying page 1 of 1

Delete Refresh

Associating Phone Book Access to Groups

You can make one or more phone books available to each group of users.

To associate phone book access to a group:

1. In Cisco TMS, go to **Phone Books > Manage Phone Books**, and then in the **Directory** pane, click the required phone book.

Information about the selected provisioning phone book is displayed in the **Workspace** pane.

2. In the **Workspace** pane, click the **Access Control** tab.



3. Click **Provisioning Directory Groups**, and then click the user group that is to have access to the selected phone book. Expand the **root** group to see subgroups.
4. If you want to grant access to all underlying phone books as well, select **Apply settings to <phone_book> and all underlying phone books**.
5. Click **Save**.

Note that while access rights will be inherited when using **Apply settings to <phone_book> and all underlying phone books**, this only applies to existing phone books, not to phone books created after performing the above procedure. When creating new phone books, access control must therefore always be specified.

Phone Book Request Handling

Phone book requests from provisioned devices *must* be handled by the same Cisco VCS or cluster that has provisioned the devices in question. If the phone book requests are being sent to a different provisioning-enabled VCS, the requests will fail, and phone books cannot be made available to the devices.

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:

Sender Address	Email address Cisco TMSPE uses as the sender email address when sending email notifications. The address appears in the From field of the recipient's email client
Subject	Subject of the email notifications. The subject appears in the Subject line of the recipient's email client.
Body	<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>
SMTP Hostname	IP-address or hostname of your SMTP (mail) server.
SMTP Port	Port number used by your SMTP (mail) server.
SMTP Username	Username to access the mail server if this is required
SMTP Password	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*.

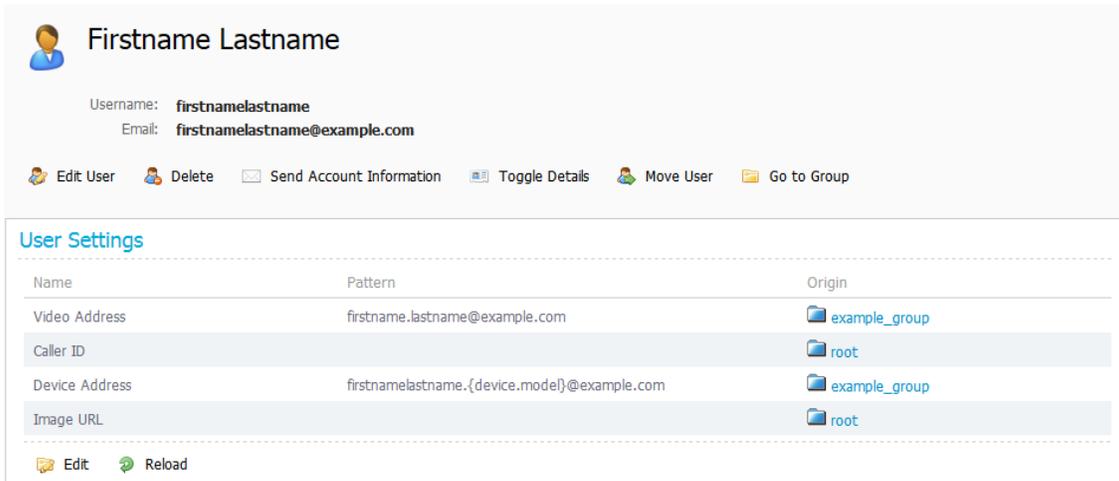
4. Click **Save**.

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 a profile picture, the name, and contact information: Username: firstnamelastname, Email: firstnamelastname@example.com. Below this is a row of 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 with columns for Name, Pattern, and Origin.

Name	Pattern	Origin
Video Address	firstname.lastname@example.com	example_group
Caller ID		root
Device Address	firstnamelastname.{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.

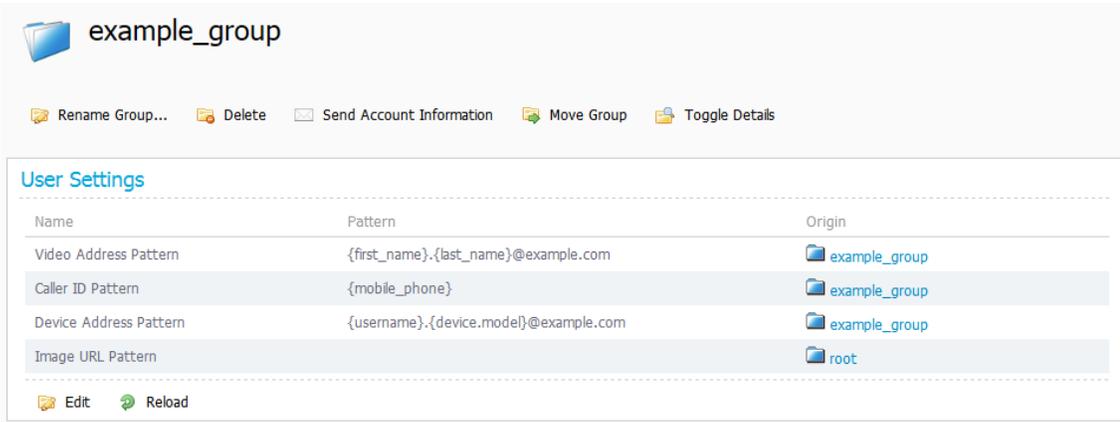
Depending on the configuration of your email server, the scheduled email should arrive in the selected recipient's inbox within a few minutes. If the email fails to be delivered, check the **Alarms** pane on the **Diagnostics** page. See [Running Cisco TMSPE Diagnostics, page 90](#).

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.

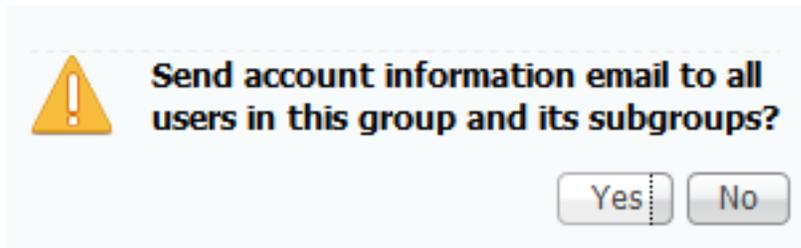
To send out account information to a group:

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 90](#).

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 52](#)

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
ISDN	Call-in participants must use ISDN for video or ISDN Audio
IP(H323)	Call-in participants must use IP(H323) for video or IP(H323) Audio
SIP	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 18](#).

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 19](#).

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 66](#) and [Setting up Host and Guest Roles in CMRs, page 64](#).

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

Like Smart Scheduler, Collaboration Meeting Room can be used independently of device provisioning and FindMe.

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 29](#).
- You must have set up a user base, see [Creating Groups and Adding Users, page 35](#).

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 Cisco VCS 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
Hostname/IP	The hostname or IP address of the TelePresence Conductor you want to connect to.
Port	The port to connect on. By default, the connection uses HTTPS on port 443.
Username	The credentials for a TelePresence Conductor administrator account with the following settings and permissions: <ul style="list-style-type: none"> - Access level: <i>Read-write</i>
Password	<ul style="list-style-type: none"> - Web access: <i>No</i> - API access: <i>Yes</i> - State: <i>Enabled</i>
Domain	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 2 Collaboration Meeting Room template configuration fields

Field	Description
Template Name	<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>
TelePresence Conductor	Select the TelePresence Conductor to use with the template from the drop-down list.
Service Preference	Select a Service Preference that has already been created on TelePresence Conductor.
SIP Alias Pattern	<p>Create a pattern for alphanumeric dialing matching Cisco VCS search rules.</p> <p>For example:</p> <pre>{username}@meeting.example.com</pre> <p>The recommended variables are:</p> <ul style="list-style-type: none"> - {username} - {email} - {office_phone} - {mobile_phone} <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>
Numeric Alias Pattern	<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>
Type	<p>Select whether to base the numeric alias pattern on:</p> <ul style="list-style-type: none"> - number ranges (<i>Generate a Number</i>). - a RegEx pattern (<i>Office Phone</i> or <i>Mobile Phone</i>).

Table 2 Collaboration Meeting Room template configuration fields (continued)

Field	Description
Number Ranges	<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"> - Both parts of the range must contain the same number of digits. For example, 01-99 will work, but 1-99 will not . - Ranges may overlap within and across templates. Duplicate numbers will not be generated. - Numbers will be assigned randomly within the range, but if there are multiple ranges, the ranges will be consumed sequentially. - A single number range cannot span more than one million numbers. <p>Example: 100000-123456, 200000-234567</p>
Prefix	Enter a string of numbers that will constitute the first part of all numeric aliases.
RegEx	<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>Example:</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"> - Given the regex <code>\d{4}</code> which will match the last four digits without any capture groups. The result will be 7890. - 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. - Given the regex <code>((?<=\.\d)\d{2}(?=\.)) (?:\.)(\d{4})</code> which will match 56.7890 with two match groups 56 and 7890. The result will be 567890.
Maximum Conference Quality	From the range of available video qualities, select the maximum quality that users will have access to when you assign them this template.
Content Sharing	Whether to allow content (presentation) sharing in rooms based on this template.

Table 2 Collaboration Meeting Room template configuration fields (continued)

Field	Description
Maximum Content Quality	<p>From the range of available qualities for content (presentation) sharing, select the maximum quality that users will have access to.</p> <p>The Maximum Content Quality setting is not applicable to CMRs that are hosted on MCU.</p>
Minimum Host PIN Length	<p>These settings control the requirements and options for PIN protection of CMRs based on the template:</p> <ul style="list-style-type: none"> – First, enter the minimum number of digits for the host role's PIN in Minimum Host PIN Length. If you leave the setting as 0, the CMR owner is not required to use a PIN for any participants. – Select whether to allow the role of guest for CMRs based on this template.: <ul style="list-style-type: none"> • The guest role has more limited privileges than the host role. • If Allow Guest Role is disabled, all participants will have the same privileges and PIN requirements as the host. – If Allow Guest Role is enabled: <ul style="list-style-type: none"> • Enter the minimum number of digits for the guest PIN in Minimum Guest PIN Length. If you leave the setting as 0, the CMR owner is not required to use a PIN for the guest role. • Choose whether to enable Guest Lobby, which means guests must wait in the lobby unless at least one host is present in the CMR. <p>For more information, see Setting up Host and Guest Roles in CMRs, page 64.</p>
Allow Guest Role	
Minimum Guest PIN Length	
Guest Lobby	
Limit Number of Participants	Choose whether to set a maximum number of participants that will be allowed in the Collaboration Meeting Room.
Maximum Participants	<p>Set a maximum number of participants to allow if Limit Number of Participants 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 Cisco TelePresence Conductor.</p>
Limit Conference Duration	<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>
Maximum Minutes	Set a maximum meeting duration in minutes if Limit Conference Duration is enabled.
Allow Multiscreen	Choose whether to allow participating telepresence systems to use more than one screen.
Maximum Screens	Set a maximum number of screens allowed per participant if Allow Multiscreen is enabled.

Table 2 Collaboration Meeting Room template configuration fields (continued)

Field	Description
Allow Cascading	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.
Number of Cascades	Set a number of MCU ports or TelePresence Server connections to reserve for cascading if enabled.
Optimize Resources	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.
Include WebEx	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 Administrative Tools > Configuration > Provisioning Extension Settings > Collaboration Meeting Room and set Allow WebEx Connections to Yes .
Advanced Parameters	Configure bridge-specific JSON objects for advanced conference parameters on creation. For examples of JSON, see Cisco TelePresence Conductor Administrator Guide .

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 66](#)

- 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

Deploying FindMe

FindMe is an integrated, but optional part of Cisco TMSPE. Provisioning and FindMe can be deployed separately or together. FindMe can also be added to a Cisco TMSPE deployment at any time.

FindMe Basics

FindMe provides the ability to specify which endpoints (video and audio-only) should ring when someone calls a user's FindMe ID. FindMe also allows a user to specify fallback devices which will be called if any of the primary devices are busy, and to specify fallback devices which will be called if none of the primary devices are answered.

An important feature of FindMe is that the administrator can configure the caller ID that is displayed on the called party's endpoint to be that of the caller's FindMe ID, rather than the ID of the caller's endpoint. This means that when that call is returned, the call will be to the FindMe ID, resulting in all that user's active FindMe location phones ringing, rather than just ringing the endpoint that happened to be the one they were at when they made the original call.

Deploying FindMe Without Provisioning

Cisco TMSPE can be used for FindMe functionality without provisioning. Performing the following configuration procedures is then recommended before starting the procedures described in this chapter:

1. Create groups and import users from an external source or add them manually, see [Creating Groups and Adding Users, page 35](#). These groups will be added to FindMe automatically when a video address pattern has been configured (see the next step), and FindMe has been enabled.
2. Assign video address patterns to these groups, see [Creating Address Patterns, page 39](#). This pattern is used to generate each user's FindMe ID, a video address that allows the user to be contacted on all of their devices. A FindMe ID can be a SIP URI, an H.323 ID, or an E.164 Alias.

You can add FindMe accounts and groups manually, but note that these users will not have access to the FindMe portal. We therefore recommend that manual accounts are only used for group accounts and any other users who will never need access to the portal. For further information about individual and group FindMe accounts, see [Individual and Group FindMe Types, page 82](#).

Defining Caller ID Patterns

Caller ID patterns are used to generate each user's callback number, which is used when a FindMe call is routed through an ISDN gateway. This ensures that a user who is contacted on their phone will see a number that they are able to call back, rather than a video address, even if the person calling is using a telepresence endpoint.

Assigning a Caller ID Pattern to Imported Accounts

This procedure applies only to FindMe accounts that are imported from the **Users** page. For manually created FindMe accounts, define the FindMe ID and caller ID while creating or editing the accounts—see [Manually Adding FindMe Accounts and Groups, page 71](#).

To assign a caller ID pattern:

1. In Cisco TMS, go to **Systems > Provisioning > Users**.
2. In the **Users and Groups** container, navigate to and click the group or user to which you want to assign a video address pattern. Information about the selected group or user is displayed under a number of panes.

- In the **User Settings** pane, click **Edit**. The **User Settings** dialog box opens.

User Settings ✕

Settings configured at the group level are inherited by all users and subgroups. Configure settings at the user level to apply them to one user only.

[\(Click for help on configuring each individual field.\)](#)

Name	Pattern	Origin
<input checked="" type="checkbox"/> Video Address Pattern	<input type="text" value="{first_name}.{last_name}@example.com"/>	example_group
<input type="checkbox"/> Caller ID Pattern	<input type="text"/>	example_group
<input checked="" type="checkbox"/> Device Address Pattern	<input type="text" value="{username}.{device.model}@example.com"/>	example_group
<input type="checkbox"/> Image URL Pattern	<input type="text"/>	root

- In the **Caller ID Pattern** field, specify the pattern that you want Cisco TMSPE to use to define callback numbers for users in the selected group, or the explicit callback number for the selected user.

You can use any of the following user attributes in the pattern:

- {office_phone}
- {mobile_phone}

- Click **OK**.

example_group

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

Example Caller ID Patterns

- {office_phone}

The following example shows how you can use regex substitutions in the pattern:

- {office_phone ['-!'=", '\+'=",' '=']}

This substitution removes unwanted characters.

Enabling FindMe in Cisco TMSPE

When you enable FindMe in Cisco TMSPE, provisioning users will be imported to the FindMe account view. Before enabling FindMe, make sure to define a video address pattern for all groups and users you want to include in FindMe:

- Groups will not be added if they do not have a video address pattern defined.
- Users without video addresses, either manually configured or based on their group's video address pattern, will not be added.

See [Creating Address Patterns, page 39](#) for further instructions on video address patterns.

To enable FindMe:

1. In Cisco TMS, go to **Administrative Tools > Configuration > Provisioning Extension Settings** and scroll down to the **FindMe** pane.

FindMe

Enable FindMe * Yes No

Provisioned Devices *

Save Cancel Restore Default

2. Set **Enable FindMe** to **Yes**.
3. From the **Provisioned Devices** field, select one of the available options depending on how you want provisioned devices to be handled:

<i>Set as default device for user's active location</i>	When a device is provisioned, add it to the list of devices in the provisioned user's FindMe account and set it as an initial device to ring at their currently active location.
<i>Add to user's device list</i>	When a device is provisioned, add it to the list of devices in the provisioned user's FindMe account.
<i>Do not include</i>	Do not add devices to the provisioned user's FindMe account as they are provisioned.

4. Click **Save**.
5. Restart the TMS Provisioning Extension Windows service following the instructions in [Restarting the TMS Provisioning Extension Windows Service, page 91](#). This must be done whenever FindMe is enabled or disabled.

Enabling FindMe will activate an icon linking to each user's FindMe portal in the top right corner of the Cisco TMS web interface.

The URL to the FindMe portal is the URL of your Cisco TMS installation with **/tmsagent/portal/** appended.

Manually Adding FindMe Accounts and Groups

You can add FindMe accounts and groups manually, but note that these users will not have access to the FindMe portal. We therefore recommend that manual accounts are only used for group accounts and any other users who will never need access to the portal. For further information about individual and group FindMe accounts, see [Individual and Group FindMe Types, page 82](#).

To add a FindMe group:

1. In Cisco TMS, go to **Systems > Provisioning > FindMe**.
2. In the **Accounts and Groups** container, click the parent of the group you want to create.
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**.

To add a FindMe account:

1. In Cisco TMS, go to **Systems > Provisioning > FindMe**.
2. In the **Accounts and Groups** container, navigate to the group into which you want to add an account.
3. Above the explorer view, click **Add Account**.
The **Add Account** dialog box is displayed.
4. Configure the fields as follows:

Display Name	Display name for the account.
Username	Username for the account.
FindMe Address	The FindMe ID for the account.
Caller ID	Callback number that is used when a FindMe call is routed through an ISDN gateway
Account Type	Select <i>Individual</i> or <i>Group</i> .

Setting up FindMe Locations and Devices

You create FindMe location and device templates if you want to provide FindMe users with locations and devices when they access the FindMe User Portal. The information you provide is passed on to and used by the configured VCSs.

To set up FindMe locations and devices, complete the following tasks:

1. [Adding FindMe Device Templates, page 72](#)
2. [Adding FindMe location templates, page 74](#)
3. [Associating Device Templates with Location Templates, page 74](#)
4. [Assigning Location Templates to Groups, page 76](#)
5. [Regenerating FindMe Locations and Devices, page 79](#)

Suggested Minimum Setup

For a minimum FindMe setup we recommend taking the following approach:

1. Enable FindMe with the **Provisioned Devices** field set to *Set as default device for user's active location*. This option results in a device being added to the FindMe portal of the associated account when the user logs in and the device is provisioned. The device is also set as an initial device to ring at the active location. See [Enabling FindMe in Cisco TMSPE, page 70](#).
2. Define one location template, for example, named `office`, and accept the default ring duration of 5 seconds. See [Adding FindMe location templates, page 74](#).
3. Assign the location template to the top-level group in the group hierarchy. See [Assigning Location Templates to Groups, page 76](#).

Adding FindMe Device Templates

Add device templates for each type of endpoint through which FindMe users can be contacted.

To add FindMe device templates:

1. In Cisco TMS, go to **System > Provisioning > FindMe**, and then click the **Device Templates** container. If one or more device templates have already been added, they are displayed in the explorer view. If no templates exist, you will see this:



[Click to add a template](#)

- Above the explorer view, click **Add Device Template**. The **Add Device Template** dialog box is displayed.

Add Device Template ✕

Display Name:

Device Type:

Device Address Pattern:

- Configure the fields as follows:

Display Name	The FindMe device name; for example, E20.
Device Type	<p>The picture to display. Select from the following:</p> <ul style="list-style-type: none"> - Video Endpoint - Telephone - Mobile Phone - Laptop - Person - Voice Mail. <p>You must select this device type for voicemail systems to ensure that the message is recorded in the correct voicebox. The setting will make the diversion header include information about the original called party.</p> <ul style="list-style-type: none"> - Video Mail - Group
Device Address Pattern	The pattern to use to create the device address or number; for example, {username}.e20@example.com.

- Click **Save**.

Adding FindMe location templates

The endpoint devices available to FindMe users may vary depending on their current location. You can add location templates to represent these variations.

For example, use location templates to represent different physical locations such as "home" or "office", as well as different circumstances such as "on vacation" or "in a meeting".

To add FindMe location templates:

1. In Cisco TMS, go to **System > Provisioning > FindMe**, and then click the **Location Templates** container. If one or more location templates have already been added, they are displayed in the explorer view. If no templates exist, you will see this:



[Click to add a template](#)

2. Above the explorer view, click **Add Location Template**. The **Add Location Template** dialog box is displayed.

Add Location Template ✕

Display Name:

Ring Duration: ▼

3. Configure the fields as follows:

Display Name	The FindMe location name; for example, office , Home Office or On the Road . This appears as a FindMe location when users configure their FindMe.
Ring Duration	This setting defines how long (in seconds) to let the devices in the current location ring before the call is forwarded to an alternative destination (busy or no answer - if configured), or is cleared.

4. Click **Save**.

Associating Device Templates with Location Templates

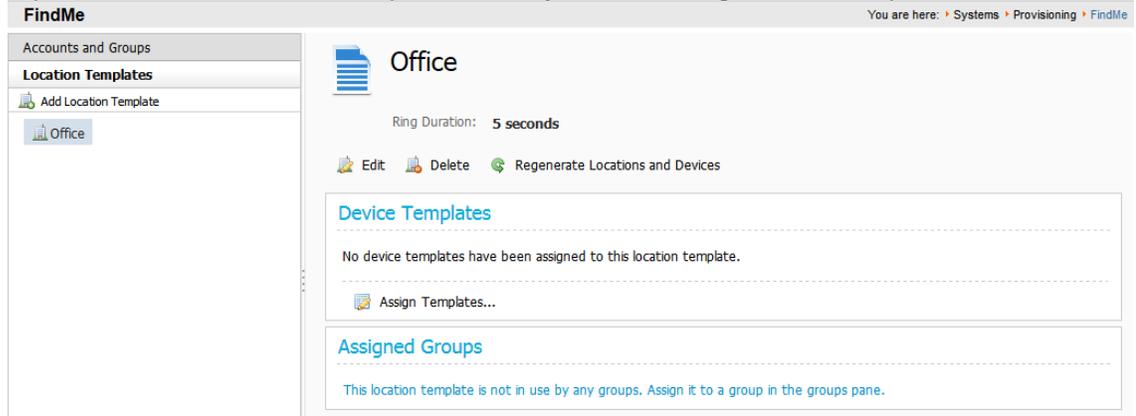
For each location template you add, you must designate at least one device that should be dialed by default whenever a user's FindMe address is contacted.

You can also specify which devices to dial:

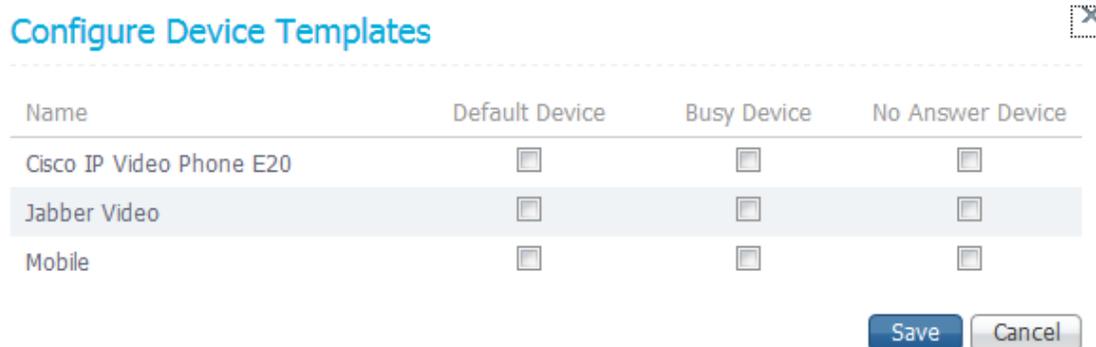
- If the designated default devices are busy.
- If a call is not answered within the location's configured ring duration.

To associate devices to a location:

1. In Cisco TMS, go to **System > Provisioning > FindMe**, click the **Location Templates** container, and then in the explorer view, click the location template to which you want to assign a device template.



2. In the **Device Templates** pane, click **Assign Templates**. The **Configure Device Templates** dialog box opens.



3. Select the appropriate check boxes to register devices as one or more of the following:

- *Default*—The initial device(s) to ring when this location is active.
- *Busy*—The device(s) to ring if the default device is busy.
- *No Answer*—The device(s) to ring if the default device is not answered.

Note that the busy and no answer devices do not forward to each other; only the default device(s) forward automatically when busy or unanswered.

4. Click **Save**.

FindMe You are here: > Systems > Provisioning > FindMe

Accounts and Groups

Location Templates

Add Location Template

Office

Office

Ring Duration: **5 seconds**

Edit Delete Regenerate Locations and Devices

Device Templates

Name	Default Device	Busy Device	No Answer Device
Cisco IP Video Phone E20	✓		
Jabber Video		✓	
Mobile			✓

Assign Templates...

Assigned Groups

This location template is not in use by any groups. Assign it to a group in the groups pane.

Assigning Location Templates to Groups

When you assign location templates to a group and apply them by regenerating the group's locations and devices, the information is passed on to and used by the configured VCSs. The location templates also becomes visible to all users in the group the next time they access their user portal. Locations are also inherited by all users in subgroups.

To assign locations to groups:

1. In Cisco TMS, go to **Systems > Provisioning > FindMe**, and click the **Accounts and Groups** container.
2. In the explorer view, click the group to which you want to assign a location template.
3. In the **Location Templates** pane, click **Assign Templates**. The **Assign Location Templates** dialog box is displayed.

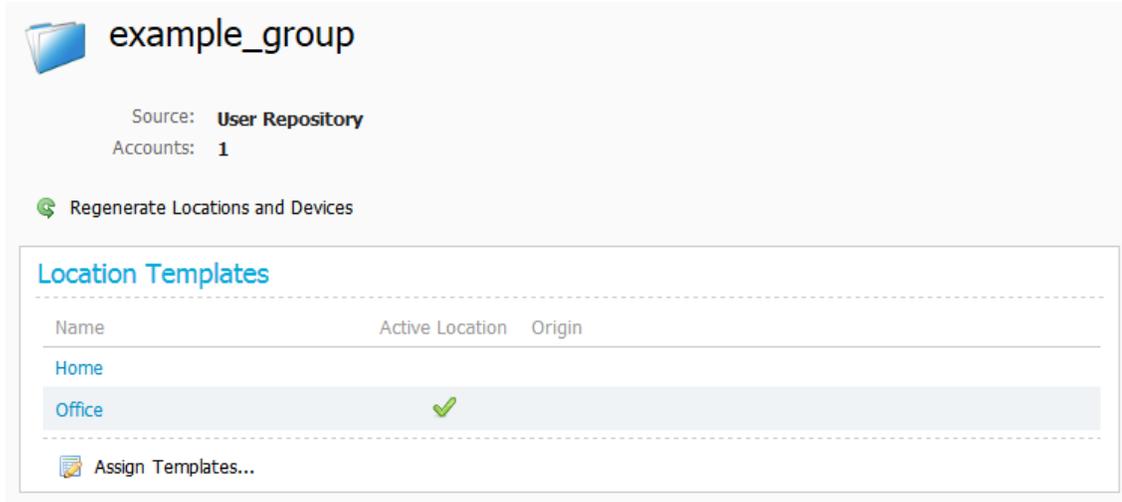
Assign Location Templates ✕

Assigned	Name	Active Location	Origin
<input type="checkbox"/>	Home	<input type="radio"/>	
<input type="checkbox"/>	Office	<input type="radio"/>	

Save Cancel

4. In the **Assigned** column, check each location you want to assign to the group.
5. Optionally, in the **Active Location** column, use the radio button to indicate the default active location for users in the group.

- Click **Save**.



- Click **Regenerate Locations and Devices...** to apply the templates for all accounts and subgroups in the current group. See [Regenerating FindMe Locations and Devices, page 79](#) for details.

Note that while you cannot assign templates directly to single users/accounts, you can access the FindMe portal on their behalf and modify their locations and devices. See [Modifying a User's FindMe Locations and Devices, page 80](#).

Setting up FindMe on Cisco VCS

The Cisco VCS must have FindMe functionality enabled so that it knows to route calls to the devices associated with a user's FindMe ID.

Check FindMe Option Key

Ensure that the Cisco VCS has the FindMe option key installed (**Maintenance > Option keys**). If it does not, contact your reseller to obtain a key.

Set up a Cluster Name

When using FindMe, you must set up the Cisco VCS with a cluster name regardless of whether it is part of a cluster.

To set up or change the cluster name:

- Go to **System > Clustering**.
- Enter the **Cluster name**:
 - If the Cisco VCS is part of a cluster, set it to the fully qualified domain name used in SRV records that address the cluster, for example "cluster1.example.com".
 - If the Cisco VCS is not part of a cluster, set it to the fully qualified domain name used in SRV records that address the Cisco VCS, for example "vcs1.example.com".
- Click **Save**.

Enable and Configure FindMe Settings

To enable and configure FindMe on the Cisco VCS:

- Go to **Applications > FindMe**.
- Set **FindMe mode** to *On*.

3. We recommend that you set **Caller ID** to *FindMe ID*. The options are:
 - *FindMe ID*: the caller ID of a call being made through this Cisco VCS is replaced with the relevant FindMe ID.
 - *Incoming ID*: the caller ID is not altered; the caller ID presented to the called endpoint will be the ID of the endpoint initiating the call.

For more details on the use of Caller ID and FindMe ID, see [Determining How to Overwrite a Caller ID with a FindMe ID, page 81](#).

4. Click **Save**.

FindMe configuration You are here: [Applications](#) > [FindMe](#)

Configuration

FindMe mode	On	?
Caller ID	FindMe ID	?
Cluster name (FQDN for Provisioning)	my.fqdn.example.com	

Sending and Returning Calls via ISDN Gateways

This section describes how to use FindMe with calls that are routed via an ISDN gateway (for example, when calling a mobile phone, or some other ISDN accessible destination).

If the Cisco VCS has **Caller ID (Applications > FindMe)** set to use the *FindMe ID*, the caller ID presented will be the user's E.164 phone number. The E.164 phone number would either have been entered manually when the user account was configured, or supplied by AD (from the Office Phone number) if Cisco TMS created the account for AD provisioned users.

If the called party returns the call (and the E.164 Alias is routed by the network to an ISDN gateway on the video network), the call will be received by the ISDN gateway and forwarded to Cisco VCS with the E.164 phone number as the called number.

Cisco VCS therefore needs to be configured to route this call to the relevant FindMe ID in order to call the user's endpoints. This can be carried out either by using another FindMe entry, or by setting up ENUM.

Using FindMe to Convert E.164 Alias's to FindMe IDs

This method uses an additional FindMe account to redirect E.164 dialed numbers to URIs.

For each user with both a URI-style or H.323 ID FindMe ID and an associated E.164 phone number, set up a second user account with:

- the **Username**, for example `123456-name.surname`
- the **FindMe ID** set to the user's E.164 phone number
- the **Principal device address** set to the FindMe ID of their main account

This is a static mapping, so the user will not ever need to log in to this second (E.164) account. Any changes to devices associated with that user are always made in their main account.

Using ENUM to Convert E.164 Alias's to FindMe IDs

Using ENUM allows incoming E.164 Alias's to be looked up in an ENUM server and the call forwarded to the URI associated with that number.

To use ENUM conversion, for each FindMe account you must set up the phone number as the ENUM address in the DNS server and then map that address to the FindMe ID for that account.

Full configuration and implementation details for ENUM are described in *ENUM dialing on Cisco VCS Deployment Guide*.

Including the ISDN Gateway Prefix in the Caller ID

It is easier to return a PSTN / ISDN call that has been received through an ISDN gateway if the Cisco VCS is configured to include the prefix of the ISDN gateway in the caller ID.

To configure the **Gateway caller ID** on the Cisco VCS:

1. Go to **Configuration > Protocols > H.323**.
2. Set the **Gateway Caller ID** as appropriate. The options are:
 - *Include prefix*: the caller ID displayed on the receiving phone is the caller's phone number prefixed by the ISDN gateway's prefix. This means the recipient can directly return the call by selecting the number and pressing return call (provided that an appropriate search rule is in place to allow calls with this prefix to be routed to the ISDN gateway). This is the recommended option.
 - *Exclude prefix*: the caller ID displayed on the receiving phone is just the caller's phone number. To return the call, the number must either be redialed or edited prefixing it with the gateway prefix so that the call can be routed via the gateway to the telephone network.

Note that if the Cisco VCS interworks an E164 H.323 call, it creates a caller ID with a domain set to the IP address of the VCS that carried out the interworking. Appropriate search rules must be created to handle the routing of these calls, or a transform implemented that converts `number@IPoFVCS` into `number@LocalSipDomain`.

Regenerating FindMe Locations and Devices

When you create or update location and device templates, the changes are not propagated out to impacted FindMe accounts until you issue the command to do so by clicking **Regenerate Locations and Devices...**

You can issue this command at a number of levels, as explained below.

Level	Description
Account	Locations and devices are regenerated only for the selected account, based on the templates available to that account. This option is useful, for example, to test the impact of changes you have made to FindMe location and device templates before regenerating at group level.
Group	Locations and devices are regenerated recursively for all accounts in the selected group and subgroups. This option is useful if, for example, the changes you make to location and device templates have an impact only on a few particular groups.
Location template	Locations and devices are regenerated recursively for all groups to which the location template is assigned. All device templates associated with the location template are also applied during regeneration. This option is useful if, for example, you make changes to a location template that is associated to a number of groups.
Device template	Devices are regenerated recursively for all impacted groups. Changes are only taken into account on existing device templates. New device templates are <i>not</i> taken into account. This option is useful if, for example, you make changes to a particular device template that is linked to a number of location templates and impacts a number of groups.

Note: Regenerating FindMe locations and devices is a background process that can take up to 30 minutes to run with very large user bases. For this reason, best results are obtained by clicking the Regenerate button once and then allowing the process to complete. Clicking the Regenerate button repeatedly will cause multiple background processes requests to be issued needlessly, and might have a detrimental impact on performance.

Accounts and Groups

To regenerate FindMe locations and devices for a specific account or recursively for all accounts in a group and subgroups:

1. In Cisco TMS, go to **Systems > Provisioning > FindMe**.
2. In the **Accounts and Groups** container, in the explorer view, navigate to the required account or group.
3. In the details area above the **Locations** pane, click **Regenerate Locations and Devices...**
4. Select whether regenerating overwrites any changes made to locations and devices by the users by clicking one of the following:
 - **Yes** to overwrite all existing locations and devices when applying the templates.
 - **No** to apply the templates without deleting or modifying user edits.

Location Templates

To regenerate FindMe locations recursively for all accounts associated with the template:

1. In Cisco TMS, go to **Systems > Provisioning > FindMe**.
2. Click the **Location Templates** pane, and then in the explorer view, click the required location template.
3. In the details area above the **Device Templates** pane, click **Regenerate Locations and Devices...**
4. Select whether regenerating overwrites any changes made to locations and devices by the users by clicking one of the following:
 - **Yes** to overwrite all existing locations and devices when applying the templates.
 - **No** to apply the templates without deleting or modifying user edits.

Device Templates

To regenerate FindMe devices recursively for all accounts associated with the template:

1. In Cisco TMS, go to **Systems > Provisioning > FindMe**.
2. Click the **Device Templates** pane, and then in the explorer view, click the required device template.
3. In the details area above the **Location Templates** pane, click **Regenerate Locations and Devices...**
4. Select whether regenerating overwrites any changes made to devices by the users by clicking one of the following:
 - **Yes** to overwrite existing devices and updates made by users when applying the templates.
 - **No** to apply the templates without deleting or modifying user edits.

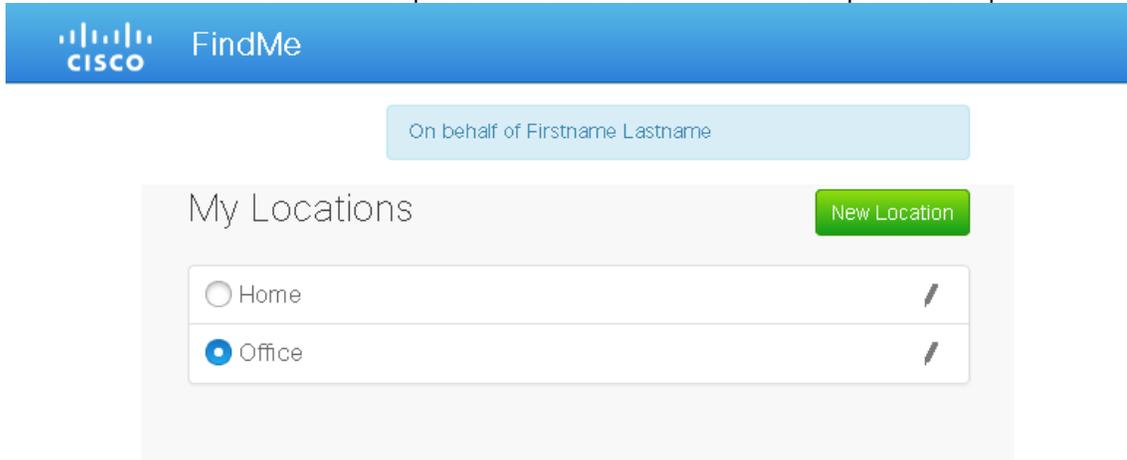
Modifying a User's FindMe Locations and Devices

It is not possible to assign location templates directly to single users/accounts. However, if a user needs help or requires a special setup, the administrator can access the FindMe portal on the user's behalf and modify their locations and devices.

Users whose FindMe accounts have been created manually cannot access their FindMe portal. The only way to modify their locations and devices is by using this procedure.

To modify a user's FindMe locations and devices:

1. Go to **Systems > Provisioning > FindMe**.
2. Open the **Accounts and Groups** container, and navigate to the FindMe account you want to modify.
3. Click **Edit in FindMe User Portal**. A separate browser tab or window will now open the user portal.



4. Add locations or make other modifications as needed.
5. Save your updates and close the browser tab. Note that you remain signed in as administrator, not as the user.

Additional Information

Determining How to Overwrite a Caller ID with a FindMe ID

Cisco VCS can only overwrite the Caller ID with a FindMe ID if:

- the call signaling passes through the Cisco VCS (or Cisco VCS cluster) that hosts the FindMe account
- the Cisco VCS can identify a FindMe as the owner of the endpoint caller ID; it can do this if the incoming caller ID provided in the call matches one of the following:
 - a FindMe device which is only found in a single FindMe account
 - a single principal FindMe device (if the same device address is associated with more than one FindMe location).

If either condition is not met, the Incoming caller ID is passed through unchanged.

FindMe in a Cisco VCS Cluster

When FindMe is used with a Cisco VCS cluster, the FindMe option key must be enabled on every Cisco VCS peer in the cluster. The FindMe database is replicated across all peers in the cluster so that FindMe functionality can be performed on any peer that a call traverses.

See [Cisco VCS Cluster Creation and Maintenance Deployment Guide](#) for more information about Cisco VCS clusters.

Microsoft Lync and the Cisco VCS B2BUA

When FindMe is used with a cluster of “Lync gateway” Cisco VCSs, each peer in the cluster registers a portion of the FindMe users to Microsoft Lync so that call loading is shared across cluster peers. (Calls from Lync to Cisco VCS are delivered by Lync to the Cisco VCS that registered the user.)

See [Microsoft Lync and Cisco VCS Deployment Guide](#) for more information.

FindMe Accounts Hosted on Hifferent Cisco VCSs in a Network

FindMe accounts can be distributed across multiple Cisco VCSs (or Cisco VCS clusters), but each individual account can be hosted on only one Cisco VCS (or Cisco VCS cluster).

For FindMe to overwrite a caller ID with the caller's FindMe ID, the call signaling must pass through the Cisco VCS (or Cisco VCS cluster) that hosts the relevant account.

Therefore, care must be taken in designing system topologies to ensure that caller ID can always be overwritten.

For example, if two users have their accounts on a VCS Control, but both are working from home on endpoints that are registered to a VCS Expressway (which has a traversal zone to the VCS Control):

- If one user calls the other user's FindMe ID, their caller ID will be overwritten by their FindMe ID, as the call signaling will go via the VCS Control (where the user account is hosted).
- If one caller calls the other user's endpoint URI directly, the call signaling will go through the VCS Expressway, but not the VCS Control. In this scenario the caller ID will not be overwritten with the FindMe ID as the signaling would not pass through the VCS Control. (It is recommended that users call FindMe IDs rather than individual device URIs.)

FindMe and Presence

The Cisco VCS aggregates presence for each of the devices associated with a user's current active FindMe location. However, it can only do this for devices whose presence is managed by a Presence Server that resides on the same Cisco VCS (or Cisco VCS cluster) that hosts the relevant FindMe account.

Therefore, we recommend that you enable the Presence Server on the same Cisco VCS (or Cisco VCS cluster) that you use to manage your FindMe accounts.

Individual and Group FindMe Types

Every FindMe profile is configured as either *Individual* or *Group*.

Individual

Individual mode assumes that the individual can only take a call on one device at a time.

- If any device in the current active location is busy, a call to this FindMe ID will be immediately forwarded to the on-busy devices.
- If no devices (in the current active location) were busy, after the specified ring duration the call will route to the on-no-answer devices.

Group

Group mode assumes that more than one person can take calls to this FindMe.

- If any device in the current active location is not busy, the non-busy devices will ring. The call is immediately forwarded to the on-busy devices only if all devices in the current active location are busy.
- If any device in the current active location is not busy, after the specified ring duration FindMe will route the call to the:
 - on-busy devices if any current active location device was busy
 - on-no-answer devices if none of the current active location device were busy

Characters Allowed in SIP URIs

The following character set is allowed in SIP URIs (further details may be found in RFC 3261):

a-z / A-Z / 0-9 / "-" / "_" / "." / "!" / "~" / "*" / "/" / "(" / ")" / "&" / "=" / "+" / "\$" / "," / ";" / "?" / "/"

If other characters are needed they must be "escaped" using "%" followed by a pair of hexadecimal digits that represents the ASCII value for the required character.

For example, "alice smith@example.com" must be encoded as `alice%20smith@example.com` (where %20 represents the space character).

FindMe Limitations

Microsoft Lync Device IDs as FindMe Devices

If **Caller ID (Applications > FindMe)** is configured to use the *FindMe ID*, so that the FindMe ID rather than the device's own endpoint ID is presented as the caller ID when making calls, Lync device IDs must not be included as a device in that FindMe. (Lync does not support the To: or From: name changing in response messages, which is how the Cisco VCS sets the Caller ID to show as the FindMe ID).

To associate video endpoints and Lync devices, the Cisco VCS's B2BUA for Lync devices should be enabled and the FindMe ID should be made the same as the Lync URI.

For further details on configuring Cisco VCS and Lync, see [Microsoft Lync and Cisco VCS Deployment Guide](#).

Phone Numbers from Active Directory (AD)

If user accounts within Cisco TMS are created from AD, the **Phone number** value is sourced from the AD Office Phone number.

For the phone number to be valid for an ISDN gateway (for the ISDN gateway to use it as a caller ID) the format of the AD Office Phone number must be acceptable to the ISDN gateway.

This typically means that the AD Office Phone number must be:

- a numeric string containing no brackets, spaces, hyphens or other non-digit characters
- a phone number which is configured by the network to terminate on the ISDN gateway
- in the correct format for the ISDN network, for example:
 - full number including country code: 441189123456
 - local number: 123456
 - extension number: 3456

Check the acceptable format with your ISDN supplier.

Maintaining Users and Devices

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 35](#)), 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 85](#).)

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.

Moving Groups Between Clusters

When moving a group causes users and FindMe accounts to get moved between two Cisco VCS clusters, you must clean up the services and perform a full synchronization on the clusters to make the users/accounts appear correctly on the VCSes:

1. In Cisco TMS, go to **Administrative Tools > Provisioning Extension Diagnostics**.
2. Run **Cleanup** on the User Preference and FindMe services.
3. Go to **Systems > Navigator** and navigate to the cluster you want to synchronize.
4. Go to the **Provisioning** tab.
5. Scroll to the bottom of the tab and click **Perform Full Synchronization**.

Repeat these steps for all clusters involved.

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.

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

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

Upgrading Software on Provisioned Devices

This process applies only to hardware endpoints, not to Jabber Video. See the *Cisco Jabber Video for TelePresence Administrator Guide* for detail on deploying and upgrading Jabber Video on Windows and Mac OS X.

Upgrading Configurations

A software upgrade is usually accompanied by a new schema that might include new configurations and modifications to existing configurations. Before you upgrade the software on provisioned devices, upload the new schema and

upgrade your configurations.

To upgrade configurations:

1. Download and add the new schema. See [Obtaining Template Schemas, page 42](#).
2. Add a new configuration template based on the new schema:
 - a. Copy the configurations from the old template. See [Adding Configuration Templates, page 44](#).
 - b. Depending on your deployment, add any new configurations needed that were not available in the previous version of the schema. Guidance on the available settings is provided in endpoint administrator documentation.
3. Assign the new configuration template or templates to your groups. See [Assigning Configuration Templates to Groups, page 47](#).

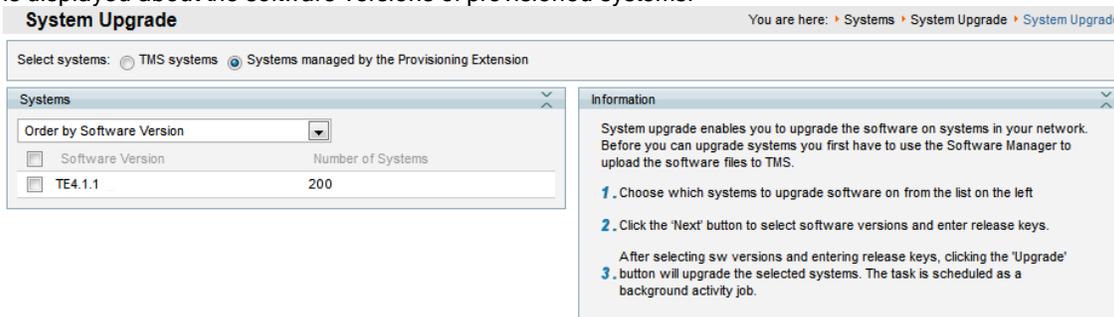
Upgrading Devices

To upgrade hard endpoints:

1. Upload the required new endpoint software versions to the software directory on the Cisco TMS server.
 - a. In Cisco TMS, go to **Systems > System Upgrade > Software Manager**.



- b. Use the **Upload New Software** button, or copy the software files manually onto the TMS server. For further information on this, see the online help.
2. In Cisco TMS, go to **Systems > System Upgrade > System Upgrade**.
3. In the **Select Systems** pane, click the **Systems managed by the Provisioning Extension** radio button. Information is displayed about the software versions of provisioned systems.



4. Use the options available to select the systems you want to upgrade, and then click **Next**. For information about the options available, see the online help.
 5. In the **Release Key** column, enter the release key for each system.
 6. From the **Software** column, select the required software package for each system.
 7. In the fields provided, select a date and time to start the upgrade process, and then click **Upgrade**.

The selected endpoints will be updated the next time a user signs in with the device and is provisioned. Note that the software package version and path specified above are saved and viewable as user-level configurations for all associated users. Go to **Systems > Provisioning > Users** and view the **User Configurations** section for each affected user.

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

The screenshot shows the 'Cisco TMS Connection' configuration form. It contains the following fields and options:

- HTTPS ***: Radio buttons for 'Yes' (selected) and 'No'.
- Connection Timeout ***: Text input field containing '10', followed by '(seconds)'.
- Receive Timeout ***: Text input field containing '60', followed by '(seconds)'.
- Username ***: Text input field containing 'administrator'.
- Password ***: Password input field with masked characters (dots).

At the bottom of the form, there are three buttons: 'Save', 'Cancel', and '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 91](#).

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.

Restoring the Databases from Backup

If restoring the databases from backup, a full synchronization with Cisco VCS clusters must be performed:

1. Go to **Systems > Navigator** and navigate to the Cisco VCS.
2. Open the **Provisioning** tab.
3. Scroll to the bottom of the tab and click **Perform Full Synchronization**.

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 91](#) 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.

Viewing Cisco VCS Communication History

On the **Provisioning Extension Diagnostics** page you can also check the recent history of attempts made by Cisco VCS to poll Cisco TMSPE for data.

All currently active Cisco VCSs are listed in the **Cisco VCS Communication** pane. The timestamp for the most recent poll is displayed in the **Last Call Time** column.

Viewing how long ago the most recent polling attempt was made may help you to identify the root cause of a problem.

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**.

Cisco VCS Logs

- Go to **Status > Logs > Network Log** to see registrations, failed registrations and other network traffic.
- Go to **Status > Logs > Event Log** for a listing of all events.
- Go to **Status > Logs > Configuration Log** to get an overview of Cisco VCS configuration changes.

Endpoint Logs

For hard endpoints, browse to their IP address to view/download logs.

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`.

Provisioning Problem Scenarios

Database Connection Failure

When Cisco TMSPE fails to connect to the database, an error message will appear in the lower right corner when accessing the **Users** page. No alarms will be raised in the diagnostics, but red indicators will show that the services are not functioning.

"The specified network name is no longer available"

If Cisco TMS is set up with Microsoft SQL Server Data Engine using the Named Pipe protocol and connections to the database start failing with the error message "The specified network name is no longer available", the required hotfixes for Windows Server have not been applied.

See [Cisco TMSPE server software and configuration requirements, page 16](#).

Log Excerpts

Look for messages like these in the log:

```
2012-10-25 15:02:24,951 [common] [JettyThread-24] ERROR U:administrator c.c.ts.mgmt.lib.api.i18n.Localizer - key Lock prevents new connection, parallell connections not supported due to underlying os operations. is not localized
```

```
2012-10-25 15:02:24,951 [common] [JettyThread-24] ERROR U:administrator c.c.t.m.l.a.i18n.ExceptionLocalizer - Key not localized: com.cisco.ts.mgmt.ur.service.userimport.settings.UserImportCommunicationException com.cisco.ts.mgmt.ur.service.userimport.settings.UserImportCommunicationException: null
```

Also look for messages containing the following or similar statements:

```
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method) ~[na:1.6.0_34]
```

```
at sun.reflect.NativeMethodAccessorImpl.invoke(Unknown Source) ~[na:1.6.0_34]
```

```
at sun.reflect.DelegatingMethodAccessorImpl.invoke(Unknown Source) ~[na:1.6.0_34]
```

```
at java.lang.reflect.Method.invoke(Unknown Source) ~[na:1.6.0_34]
```

User Import Fails

If you have configured a nightly user import from AD or LDAP and it fails, a ticket will be raised. You are most likely trying to import users logged in with a service account in AD that has an expired password.

To address the issue:

1. Ensure that all prerequisites for user import are in place. See [User import requirements, page 20](#). Pay special attention to the user account and password.
2. Do a manual import or wait for the scheduled import.

Email Sending Failure

If account information email is not reaching the recipients:

- Verify that the SMTP server, port, username, and password are correctly configured in the [Configuring Email Settings, page 50](#).
- Check whether antivirus software is preventing email from being sent. Some antivirus applications automatically block all mass sending of email.

Cisco VCS Reports Data Import Failure

If Cisco VCS raises a Cisco TMS ticket with the alarm "TMS Provisioning Extension services data import failure", there is a problem with the data format or the number of entries received from Cisco TMSPE.

"Would cause the VCS to exceed internal table limits"

A Cisco VCS cluster of any size supports the import of:

- 10,000 users for provisioning
- 10,000 FindMe accounts
- 15 devices for each user
- 200,000 phonebook entries

If the above alarm is raised, the maximum number of users, FindMe accounts, or phone book entries has been exceeded.

Corrective actions: First verify that the number of entries reported is correct:

1. In Cisco TMS, go to **Administrative Tools > Provisioning Extension Diagnostics**.
2. Next to the relevant service (Users, Phone Book, or FindMe), click **Cleanup**.
3. Go to **Systems > Navigator** and navigate to the Cisco VCS.
4. Open the **Provisioning** tab.
5. Scroll to the bottom of the tab and click **Perform Full Synchronization**.

If the alarm was due to data duplication in Cisco TMSPE, the synchronization should now complete successfully.

If Cisco VCS limitations are still exceeded, view the Cisco VCS event log for details.

- Move groups to a cluster with available capacity if user and/or FindMe limitations are exceeded.
- Reduce the total number of phone book entries in Cisco TMS if it exceeds 200 000.

"Unrecognized data format"

If the ticket reports that "One or more records imported from the TMS Provisioning Extension services have been dropped due to unrecognized data format", the problem is one of the following:

- The record is not in a recognized format
- A mandatory field, for example FindMe URI, is either empty or missing from the record
- A field contains the wrong type of data/an invalid value

Corrective actions:

1. See the Cisco VCS event log for details.
2. Correct the errors based on the event log.

Users Get "Out of licenses" Message

If users get an error message saying "Out of Licenses" when signing in to Cisco Jabber Video for TelePresence, this usually indicates that the maximum concurrent number of users has been exceeded. However, if this happens immediately after setting up Cisco TMSPE, the message may be due to a misconfiguration.

To check this:

1. Go to **Systems > Navigator**.
2. Select the Cisco VCS the client is trying to sign into and go to the **Provisioning > Devices** pane.

3. In the **Devices** pane, make sure **Enable Service** is selected.

For further instructions, see [Configuring Cisco VCS via Cisco TMS](#).

Signing in Fails When No Template Available

A device will not be able to sign in for provisioning if no template exists for the type of device. If no template exists for its version, Cisco TMSPE will fall back to the latest template available for earlier versions. Note that Cisco TMSPE cannot fall back to a newer template if none exists for the specific version of device or earlier.

If a particular type of device fails to sign in:

1. In Cisco VCS, go to **Status > Logs > Event Log**.
2. If the log contains an error message similar to this, Cisco TMSPE has not been set up with a template for the device:

```
provisioning: Level="ERROR" Detail="Failed to provision user" User-URI="[user's SIP URI]" Reason="No provisioning template document found" Device-model="[device]" Device-version="[software version]"
```

For instructions on adding templates, see [Setting up Configurations for Provisioned Devices, page 42](#).

Warning Displayed When Uploading Configuration Schema

If a warning appears in the Cisco TMSPE administrative interface when uploading a schema, this may be due to a web server configuration issue where HTTP PUT requests are stopped by IIS:

1. Open IIS Manager on the Cisco TMSPE server.
2. Select the Cisco TMSPE web application (`<machinename>/Sites/Default Web Site/tmsagent`).
3. In the middle pane, double-click on **Request Filtering**.
4. In the same pane, select the **HTTP Verbs** tab.
5. Ensure that PUT is set to `Allowed=True`.

If PUT is already enabled for the web application, check whether server-wide settings are overriding individual webapp configurations.

Note that this issue is only seen when WebDAV Publishing is an IIS Role Service.

No Phone Books Received

If one or more provisioning users are not receiving phone books on their devices:

- Verify that access control is correctly set up for the user(s). See [Associating Phone Book Access to Groups, page 49](#).
- Ensure that phone book requests from provisioned devices are handled by the same Cisco VCS or cluster that has provisioned the devices in question. If the phone book requests are being sent to a different provisioning-enabled VCS, the requests will fail, and phone books cannot be made available to the devices.

Update CMR templates to Support Multiparty license

When Cisco TMSPE and Conductor are upgraded to support Multiparty license. The CMR templates associated with the Conductor that support Multiparty license must follow the below mentioned steps:

1. Edit CMR templates.
2. Select the required Multiparty License Mode.
3. Click the **Save** button to update the templates.

Portal Troubleshooting

Cannot Access FindMe or Smart Scheduler

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

Using Search History to Diagnose FindMe Issues

Looking at search history (on the Cisco VCS or Cisco VCS cluster that hosts the relevant user account) is usually the best place to start diagnosing FindMe-related problems.

The search history shows the search for the FindMe ID and then how User Policy forks the call to look at all the devices in the currently active location. The results of the searches for each device are also shown.

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 91](#) 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.

Removing Provisioning From a Cisco VCS

If provisioning is no longer required or if provisioning was accidentally enabled on a VCS Expressway, follow the instructions below:

In Cisco VCS:

1. Go to **Maintenance > Option keys**.
2. Select the **Device Provisioning** option key.
3. Click **Delete**.

Document revision history

Date	Description
July 2018	Release of Cisco TMSPE 1.13.
December 2017	Release of Cisco TMSPE 1.12.
September 2017	Release of Cisco TMSPE 1.11.
April 2017	Release of Cisco TMSPE 1.10.
December 2016	Release of Cisco TMSPE 1.9.
August 2016	Release of Cisco TMSPE 1.8.
April 2016	Release of Cisco TMSPE 1.7.
September 2015	Release of Cisco TMSPE 1.5.
January 2015	Release of Cisco TMSPE 1.4.
November 2014	Added summary of license requirements. Updated tested Java versions to include Java 7 update 71.
September 2014	Release of Cisco TMSPE 1.3.
January 2014	Added information on user access to Smart Scheduler.
December 2013	Updated for the release of Cisco VCS X8.1.
December 2013 12 11 . Clarified in da	Added database server requirements section in Prerequisites, see SQL Server software and permission requirements, page 17 .
October 2013	Updated information on editing ongoing meetings using Smart Scheduler.

Date	Description
September 2013	Added and updated browser requirements, previously only located in FindMe User Guide. Updated Java requirements to reflect that Cisco TMSPE has been tested with Java 7, update 40. Clarified in database maintenance section that renaming the database is not supported.
2013-06-17	Updated to reflect the release of Cisco TMS 14.2.2, which is now a requirement for deployments using Smart Scheduler. See Cisco TelePresence Management Suite Release Notes (14.2.2) for details.
2013-05-15	Added cautionary note about open issue CSCu74973; installing with a blank, manually created database does not work with Cisco TMSPE 1.1. For workaround, see Database location, page 19 .
2013-04-24	Release of Cisco TMSPE 1.1.
2012-12-17	Updated document to cover deployment with Cisco TMS 14.1. Migration no longer supported, must be performed using Cisco TMS 13.2
2012-10-30	Clarified Java 6 requirements, added related troubleshooting item. Added IIS redirection limitation to Cisco TMS requirements. Modified endpoint recommendations to include Cisco Jabber Video for TelePresence 4.2. Specified that database name is case sensitive. Added information about FindMe URL.
2012-09-13	Clarified SQL prerequisites in requirements section. Added phone book and template upload troubleshooting scenarios.
2012-08-07	Added support for Cisco VCS X7.2.
2012-07-06	Added troubleshooting scenarios for certificate validation error and sign-in failure when no template is available.
2012-05-10	Added troubleshooting item for SQL Server Browser not running. Removed un-needed installation workaround for default database instances.
2012-04-27	Release of Cisco TMSPE 1.0.

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

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.

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.

© 2018 Cisco Systems, Inc. All rights reserved.

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)