



Cisco TelePresence Management Suite Provisioning Extension with Cisco Unified CM

Deployment Guide

Cisco TMSPE 1.2
Cisco TMS 14.4
Cisco Unified CM 10.0 or 9.1
TelePresence Conductor XC2.3

D15110 01

May 2014

Contents

Introduction	5
This deployment guide	5
Related documents	5
Prerequisites and recommendations	6
Estimating your deployment size	6
Hardware requirements	6
Regular deployment	7
Large deployment	7
Recommended hardware and virtualization for large deployments	8
Cisco TMSPE server software and configuration requirements	9
SMTP server requirements	9
SQL Server software and permission requirements	9
WebEx Enabled TelePresence requirements	10
Collaboration Meeting Room requirements	10
Cisco TelePresence Conductor	10
Cisco Unified Communications Manager	10
Required security permissions	11
For installation	11
For operation	11
Information needed during installation	11
Cisco TMS username and password	11
Database information	11
Database location	12
User import requirements	12
Service account	12
Secure connection	12
Active Directory	12
LDAP	13
Browser requirements	13
Administrator interface	13
User portal	13
Best practices for deployment	13
Automate user creation and management with AD/LDAP	13
Use secure communication	13
Installing Cisco TMSPE	14
Installing Cisco TMSPE with a redundant Cisco TMS setup	14
Upgrading from previous versions	14
If the server is running Java 7	14
If the server is running Java 6	14
Performing a new installation	15
Enabling Cisco TMSPE	15
Setting up users	17
Creating groups and adding users	17
Setting up groups	17
Importing users from external directories	17
Adding users manually	20

Configuring and sending account information	21
Configuring email settings	21
Sending account information to a single user	23
Sending account information to all users in a group	23
Deploying Smart Scheduler	25
Best practices and limitations	25
Booking limitations	25
User access to Smart Scheduler	26
Access rights and permissions	26
Time zone display	27
WebEx booking	27
How Smart Scheduler works	28
Deploying Collaboration Meeting Rooms	29
What are Collaboration Meeting Rooms?	29
Room size and quality	29
PIN protection	29
How Collaboration Meeting Rooms are created	29
Differences from TelePresence Conductor-created conferences	29
Setting up Collaboration Meeting Room	30
Before you start	30
Connecting to TelePresence Conductor	30
Creating templates	31
Applying templates to groups	33
Making changes that affect Collaboration Meeting Room	34
Modifying or replacing the template for a group	34
Deleting templates	35
Deleting users	35
Moving users between groups	35
Touch tones and DTMF	35
Maintaining users	36
Synchronizing user data	36
Mapping of LDAP and AD fields	36
Testing a manual synchronization	37
Running a manual synchronization	37
Moving users and groups	37
Moving user accounts imported from external sources	37
Searching for user accounts	37
Renaming groups and user accounts	38
Updating Cisco TMS connection details	38
Maintaining the databases	40
Backing up the databases	40
Moving or renaming the databases	40
Troubleshooting	41
Running Cisco TMSPE diagnostics	41
Running a health check	41
Viewing system status	42
Restarting the TMS Provisioning Extension Windows service	42
Logs	42

Cisco TMSPE and Cisco TMS logs	42
Troubleshooting the installation	43
Checking the installation log	43
Unable to establish SQL connection through Java runtime... ..	43
Unable to find valid certification path to requested target	43
Portal troubleshooting	44
Cannot access FindMe or Smart Scheduler	44
Uninstalling Cisco TMSPE	45
Notices	46
Accessibility notice	46
Technical support	46

Introduction

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

- Smart Scheduler, a web-based telepresence scheduling tool for end users.
- Collaboration Meeting Room, personal telepresence bridges for unscheduled meetings.

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

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

This deployment guide

This guide covers the deployment and maintenance of Cisco TMSPE 1.2 with Cisco TMS version 14.4 and Unified CM.

The document provides:

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

Related documents

All documentation for the latest version of Cisco TMSPE can be found at

http://www.cisco.com/en/US/products/ps11472/tsd_products_support_series_home.html.

Title	Link
<i>Cisco TMSPE Release Notes</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>How to enable Windows Installer logging</i>	http://support.microsoft.com/kb/223300
<i>Distinguished Names</i>	http://msdn.microsoft.com
<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.

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	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 controlled systems ■ < 1800 concurrent participants ■ < 250 concurrent ongoing scheduled conferences
Cisco TMSXE	< 50 endpoints bookable in Microsoft Exchange	< 1800 endpoints bookable in Microsoft Exchange
Cisco TMSPE	<ul style="list-style-type: none"> ■ < 1000 Collaboration Meeting Rooms ■ < 2000 Cisco VCS-provisioned users 	<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

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

	Requirement
CPU	2 cores (Xeon 2.4 GHz or larger), dedicated
Memory	8 GB, dedicated
Disk space provided on server	60 GB

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

Microsoft SQL Server

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

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

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

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

Cisco TMSXE server

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

Recommended Cisco TMS configuration changes

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

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

Recommended hardware and virtualization for large deployments

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

Hardware

Server	Cisco UCS C220 M3S Rack Server
CPU	2 x Intel Xeon Processor E5-2430 v2 (2.50 GHz)
Disk	8 x 146GB 6G SAS 15K RPM SFF HDD/hot plug/drive sled mounted, in a RAID-6 configuration. Part number: A03-D146GC2.
Disk controller	LSI MegaRAID 9265-8i 6Gb/s
Memory	4 x 8 GB/1600 MHz
Hypervisor software	VMware ESXi 5.1 hosting the three virtual machines with the specifications described below.

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 TMSPE1.2 requires Cisco TMS 14.4. ■ For complete Cisco TMS requirements, see Cisco TelePresence Management Suite Installation and Upgrade Guide. Note that trial versions of Cisco TMS cannot activate this extension. ■ See hardware recommendations below. <p>Users of earlier versions of Cisco TMS must refer to the deployment guide and installation guide for their version.</p>
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. ■ If using the Named Pipes protocol for SQL database connection, the following security updates/hotfixes to Windows Server are required for Windows Server 2008 R2: http://support.microsoft.com/kb/2194664 and http://support.microsoft.com/kb/2444328 Note that the default connection protocol is TCP/IP. If this protocol is used, no hotfixes are required.
Java	<p>Cisco TMSPE has been tested with Java 7, update 51, 32-bit and 64-bit versions. 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.</p>

No support for multiple network cards

Multiple network cards on the Cisco TMS server are not supported. Cisco TMSPE cannot use multiple network cards on a server and will only bind to the first available network interface.

SMTP server requirements

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

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

SQL Server software and permission requirements

A complete installation of Cisco TMSPE creates three databases:

- **tmspe**
- **tmspe_vmr**
- **tms_userportal**

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

User and database creation

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

- Automatic setup, but with security limited role. Ask your SQL server administrator to create an SQL user and login that has the dbcreator and securityadmin server roles. This account will be the service account for Cisco TMSPE. When prompted for SQL Server credentials during installation, enter the username and password for that account. Cisco TMSPE will create the `tmspe/tmspe_vmr/tms_userportal` databases automatically using the server defaults, assign itself as the owner and continue to use the supplied account to access the databases after installation.
- Manual database creation, max security limited role. Ask your SQL server administrator to create:
 - Empty databases named `tmspe`, `tmspe_vmr`, and `tms_userportal` in the same instance as `tmsng`, with database collation `Latin1_General_CI_AI` (case insensitive and accent insensitive). 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.

WebEx Enabled TelePresence requirements

In order to use Cisco TMSPE to book 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 WebEx Enabled TelePresence with or without single sign-on, see [WebEx Enabled TelePresence Configuration Guide](#).

Collaboration Meeting Room requirements

Cisco TelePresence Conductor

TelePresence Conductor version XC2.3 is required.

Cisco Unified Communications Manager

Unified CM 9.1.x or 10.0.x is required.

Routing requirements

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

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

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

Required security permissions

For installation

The following security permissions are required for installing Cisco TMSPE:

Application	User Privilege
Cisco TMS Windows 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 [p.11] for further details.

For operation

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

Application	User Privilege
Cisco TMS SQL server instance	<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.

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 `tmsg` 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 `tmsg` 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 \[p.11\]](#) for appropriate operation permissions.

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 1.2 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 10 and above
- Firefox 29 and above
- Google Chrome 34 and above
- Safari 7 and above for Mac OS X and iPad

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

Best practices for deployment

Automate user creation and management with AD/LDAP

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

For Active Directory import to work:

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

Use secure communication

Cisco TMSPE requires a secure connection with HTTPS. When you upgrade or install Cisco TMS, the installer enables HTTPS communication. We strongly recommend using valid certificates. Cisco TMS will otherwise offer to create a self-signed certificate.

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 \[p. 15\]](#).
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. Change the provisioning mode on all servers only after completing the above steps. See [Enabling Cisco TMSPE \[p. 15\]](#).

We also recommend probing `/tmsagent/tmsportal` to check that the service is responding.

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

Upgrading from previous versions

If the server is running Java 7

To upgrade from Cisco TMSPE 1.1 or 1.0 if Java 7 is already installed on the server:

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 installer instructions.

Any existing provisioning and FindMe configurations will be kept when upgrading.

If the server is running Java 6

To upgrade from Cisco TMSPE 1.1 or 1.0 if the server is still running Java 6:

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

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 location and instance.
 - i. 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.
 - ii. Fill in the necessary credentials.
 - iii. Click **Next**.
 - f. Click **Install** to begin the installation. Click **Back** to review or change installation settings.
 - g. When the installation is complete, click **Finish** to exit the **Setup** window.
6. Re-enable virus scanning software.

Enabling Cisco TMSPE

After completing the installation:

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

The screenshot shows the 'General Settings' page in Cisco TMS. The breadcrumb trail at the top right reads 'You are here: Administrative Tools > Configurations'. The 'General Settings' section is active. The 'Provisioning Mode' dropdown menu is open, showing three options: 'No', 'Provisioning Extension', and 'Provisioning Extension'. The 'Provisioning Extension' option is selected and highlighted in blue. 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 (order of name to use), 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:
 - o **Systems > Provisioning > Users**. If this page reports a problem connecting to User Repository, the database connection is not working. See [Troubleshooting the installation \[p.43\]](#).
 - o **Systems > Provisioning > Devices**
 - o **Systems > Provisioning > FindMe**
Note that **Systems > Provisioning > FindMe** will be displayed with an error message if when/if FindMe has been enabled.
 - o **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 \[p.43\]](#) for further information.

Setting up users

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

Creating groups and adding users

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

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

Setting up groups

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

To add a group:

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

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

Importing users from external directories

Before you start

1. Ensure that the intended directory source is supported, see [User import requirements \[p.12\]](#).
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.

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.

The screenshot shows the user management interface for a group named "example_group". At the top, there is a folder icon and the group name. Below this, there are several action buttons: "Rename Group...", "Delete", "Send Account Information", "Move Group", and "Toggle Details".

The "User Settings" pane contains a table with the following data:

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

Below the table are "Edit" and "Reload" buttons.

The "User Import" pane shows a radio button selected for "No user import has been configured for this group." and a "Configure" button.

- In the **User Import** pane, click **Configure**.
- If you want to copy user import settings from the parent group as a starting point, click **Copy from parent**.
- 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:

- 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.
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 \[p.36\]](#).

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 *	<input type="text" value="5000"/>	(milliseconds)
Filter Template *	<input type="text" value="{&(objectCategory=person)(sAMAccountType=80530)"/>	
Follow Referrals *	<input checked="" type="radio"/> Yes <input type="radio"/> No	

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 \[p.20\]](#).

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.
6. Click **Save**.

Configuring and sending account information

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

Configuring email settings

To configure email settings:

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

Account Information Email

Sender Address *

Subject *

Body *

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




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

SMTP Hostname *

SMTP Port *

SMTP Username

SMTP Password

 Save  Cancel  Restore Default

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

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 user's name, and their contact information: Username: firstnamelastname and Email: firstnamelastname@example.com. Below this, there are several action buttons: Edit User, Delete, Send Account Information, Toggle Details, Move User, and Go to Group. The 'User Settings' section is expanded, showing a table with columns for Name, Pattern, and Origin. The table contains the following data:

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, there 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 \[p.41\]](#).

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.

example_group

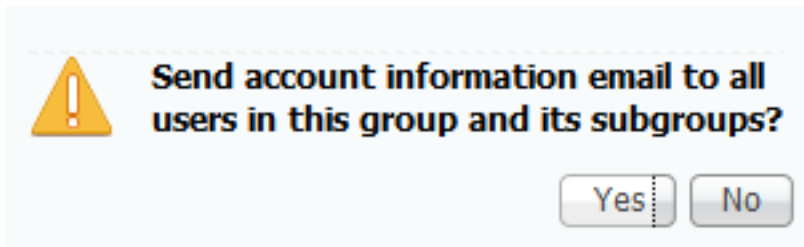
Rename Group... Delete Send Account Information Move Group Toggle Details

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

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



- 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 \[p.41\]](#).

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 \[p.23\]](#)

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 WebEx Enabled TelePresence 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 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 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.

Modifying ongoing meetings

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

When modifying any meeting:

- if the meeting is using an MCU that does not support WebEx, WebEx may not be added, as the meeting would have to be disconnected and re-routed for this to work.
- extending the meeting will fail if it creates a booking conflict for any of the participants.

When modifying single meetings, including meetings in a series:

- editing the start time will not work and Cisco TMS will throw an exception.
- 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.

When *deleting* a recurrent series while a meeting in the series is ongoing, the ongoing meeting will end.

When *modifying* a recurrent series while a meeting in the series is ongoing, the ongoing occurrence is turned into a single meeting, separate from the series, and:

- 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.

This is also where users can set their preferred display format for time and date, which is stored in the browser's cookies.

WebEx booking

With Smart Scheduler users can book:

- WebEx Enabled TelePresence 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 WebEx Enabled TelePresence has been set up with Cisco TMS, see [WebEx Enabled TelePresence requirements \[p.10\]](#).

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 \[p.11\]](#).

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

PIN protection

Access to rooms can be restricted by the use of a PIN code. The administrator determines whether a PIN is required and the minimum number of digits.

Note that changing the PIN requirements for CMRs will cause confusion for users and as administrator you can send an email to prompt the users about the change.

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.

The administrator sets up a user base and configures entitlement for one or more groups of users in Cisco TMSPE that will be allowed to have Collaboration Meeting Room. The address pattern and available parameters for each user's CMR are determined by a CMR template, which is linked to a Service Preference on TelePresence Conductor. The administrator sets up the CMR templates and applies them per group in Cisco TMSPE.

When initiated by a user, Cisco TMSPE creates a CMR on TelePresence Conductor based on the template for the user's group and reserves an alphanumeric and/or numeric video address for each user's CMR.

The CMR is 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 Room.

Setting up Collaboration Meeting Room

Before you start

- Cisco TMSPE must be installed and enabled in Cisco TMS.
- A user base must be set up, see [Creating groups and adding users \[p. 17\]](#).
- Each TelePresence Conductor system to be used must be set up with one or more populated bridge pools and one or more Service Preferences. It is only possible to use Cisco TelePresence MCUs or Cisco TelePresence Servers.
If setting up a new deployment, follow the instructions in [Cisco TelePresence Conductor with Unified CM Deployment Guide](#), omitting tasks to create conference templates, aliases, and auto-dialled participants.

Connecting to TelePresence Conductor

It is only possible to connect 30 TelePresence Conductors.

Connect only to one TelePresence Conductor from each cluster of conductors.

On each TelePresence Conductor:

1. Go to **Users > Administrator accounts**.
2. Click **New**.
3. Add a new user exclusively for Collaboration Meeting Room, 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.

Field	Description
Username	The credentials for a TelePresence Conductor administrator account with the following settings and permissions:
Password	<ul style="list-style-type: none"> • Access level: <i>Read-write</i> • 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 1: 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.

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

Field	Description
SIP Alias Pattern	<p>Create a pattern for alphanumeric dialing.</p> <p>For example:</p> <p><code>{username}@meeting.example.com</code></p> <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	Whether to add a numeric alias for each room in addition to the alphanumeric alias. Check to display the below settings.
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 or Mobile Phone</i>).
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>

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

Field	Description
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.
Maximum Content Quality	From the range of available qualities for content (presentation) sharing, select the maximum quality that users will have access to.
Limit Number of Participants	Choose whether to set a maximum number of participants that will be allowed in the Collaboration Meeting Room.
Maximum Participants	Set a maximum number of participants to allow if Limit Number of Participants is enabled. 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 .
Limit Conference Duration	Choose whether to set a maximum duration for meetings in the CMR. Enable this setting to prevent meetings where participants forget to disconnect, so that the meeting continues.
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.
Require Conference PIN	Choose whether a PIN must be set for the CMR.
Minimum Length	If requiring users to secure their room with a PIN, specify the minimum number of digits required.
Optimize Resources	Select whether to allow TelePresence Conductor to free up any allocated resources not used by participants once the meeting has started.
Advanced Parameters	Choose whether to set advanced parameters.
Advanced Parameters	Configure bridge-specific JSON objects for advanced conference parameters on creation. For examples of JSON, see Cisco TelePresence Conductor Administrator Guide .

- 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.

Making changes that affect Collaboration Meeting Room

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.

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.

- 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.

- 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.
- 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

It is possible for users to enter touch tones for auto-connections.

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

Maintaining users

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

Synchronizing user data

When you configure the import of user account data from external sources (see [Creating groups and adding users \[p.17\]](#)), 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 \[p.37\]](#).)

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
objectGUID	entryUUID	external_id	
sAMAccountName	cn	Username	username
mail	mail	Email	email
title	title	Title	
givenName	givenName	First Name	first_name
sn	sn	Last Name	last_name
company	company	Company	
department	department	Department	
telephoneNumber	telephoneNumber	Office Phone	office_phone
mobile	mobile	Mobile Phone	mobile_phone
displayName	displayName	Display Name	display_name

Testing a manual synchronization

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

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

Running a manual synchronization

To run a manual synchronization:

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

Moving users and groups

To move groups and manually created accounts:

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

Moving user accounts imported from external sources

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

Searching for user accounts

To search for a user account:

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

- To identify the group to which the account belongs, click the **Go to group** button localized on top of the left pane.

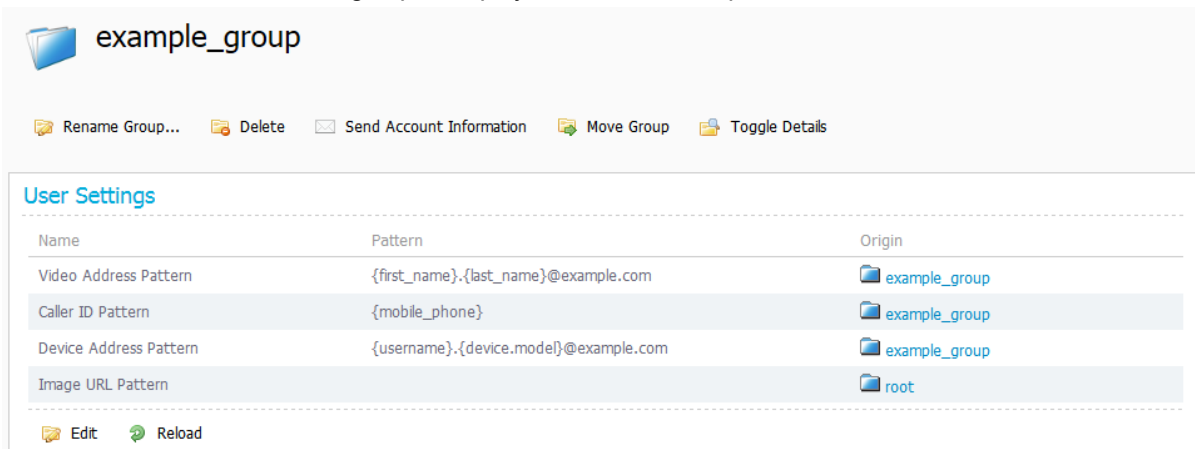
Renaming groups and user accounts

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.

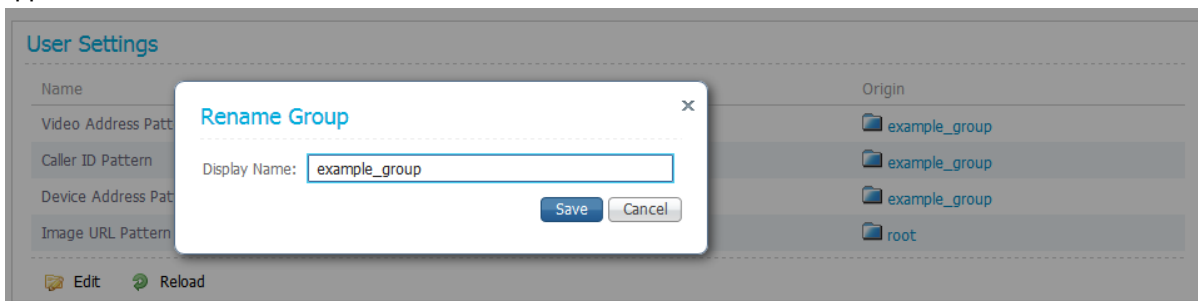
To change the display name of users and groups:

- In Cisco TMS, go to **Systems > Provisioning > Users**.
- 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.



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



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




Updating Cisco TMS connection details

To update connection details for Cisco TMS:

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

Cisco TMS Connection

HTTPS *	<input checked="" type="radio"/> Yes	<input type="radio"/> No	
Connection Timeout *	<input type="text" value="10"/>		(seconds)
Receive Timeout *	<input type="text" value="60"/>		(seconds)
Username *	<input type="text" value="administrator"/>		
Password *	<input type="password" value="••••••••"/>		

 Save  Cancel  Restore Default

3. Modify settings as desired.
4. Click **Save**.
5. Restart the Provisioning Extension service, see [Restarting the TMS Provisioning Extension Windows service \[p.42\]](#).

Maintaining the databases

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

Backing up the databases

We recommend backing up the Cisco TMSPE databases regularly.

Moving or renaming the databases

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

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

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

After updating the database instance, restart the Windows service for the connection settings change to take effect, see [Restarting the TMS Provisioning Extension Windows service \[p.42\]](#) 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.

The screenshot shows the 'Run Health Check' interface. At the top right, it says 'Version: 1.2.0.24'. Below the title bar, there are two main sections: 'Alarms' and 'System Status'.

Alarms Table:

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 Table:

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 color-coded status circles. Red circles indicate an error or warning.
3. To attempt to fix a problem, click the corresponding button:
 - **System Status**: click **Cleanup**.
This action cleans up the delta table in the database, which holds information about data changes such as user and group updates. The accumulation of changes in the delta table can cause the database to grow over time.
 - **User Import Status**: click **User Import**.
This action initiates a full import from the user repository to the target service.
 - **Device Import Status**: click **Device Import**.
This action initiates a full import from the device repository to the target service.
4. View the Cleanup Status circle to confirm that the problem has been fixed.
Typically, the status changes to orange indicating it is awaiting processing, to a cog wheel indicating that the task is in progress, to a green circle indicating that the status is now OK.

Restarting the TMS Provisioning Extension Windows service

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

To restart the service:

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

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

Logs

Cisco TMSPE and Cisco TMS logs

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

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

Troubleshooting the installation

Checking the installation log

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

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

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

Unable to establish SQL connection through Java runtime...

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

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

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

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

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

Unable to find valid certification path to requested target

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

1. Click **Cleanup**.
2. After a few minutes, run a health check to refresh the information display.
3. If the circle is still red, check the log. If the `tmsprovisioningextension.log` file contains the following line:

```
Caused by: javax.net.ssl.SSLHandshakeException:  
sun.security.validator.ValidatorException: PKIX path building failed:  
sun.security.provider.certpath.SunCertPathBuilderException: unable to find  
valid certification path to requested target
```

- a. Place your certificate file somewhere on the Cisco TMS server.
- b. Update the JRE keystore from `JRE_HOME\bin` on the server using the following command:

```
keytool -import -alias myprivateroot -keystore ..\lib\security\cacerts -  
file c:\hello.cer
```
- c. Enter the password for the keystore when prompted. The default password is `changeit`.

Portal troubleshooting

Cannot access FindMe or Smart Scheduler

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

Uninstalling Cisco TMSPE

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

Using the installer

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

A log of the uninstallation will be created in:

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

Note that starting the uninstallation process stops the Windows service, and that cancelling the uninstallation will not restart the service. See [Restarting the TMS Provisioning Extension Windows service \[p.42\]](#) 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 2008 and later versions.

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

Technical support

If you cannot find the answer you need in the documentation, check the website at www.cisco.com/cisco/web/support/index.html where you will be able to:

- Make sure that you are running the most up-to-date software.
- Get help from the Cisco Technical Support team.

Make sure you have the following information ready before raising a case:

- Identifying information for your product, such as model number, firmware version, and software version (where applicable).
- Your contact email address or telephone number.
- A full description of the problem.

To view a list of Cisco TelePresence products that are no longer being sold and might not be supported, visit: www.cisco.com/en/US/products/prod_end_of_life.html and scroll down to the TelePresence section.

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 NON-INFRINGEMENT 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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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.

© 2014 Cisco Systems, Inc. All rights reserved.