Cisco TelePresence Management Suite Provisioning Extension

Deployment Guide

Cisco TMSPE 1.1
Cisco TMS 14.2 or 14.3
Cisco VCS X8.1

D14941 15

January 2014

Contents

Introduction

Cisco TMS Provisioning Extension (Cisco TMSPE) is a provisioning application for Cisco TelePresence Management Suite (Cisco TMS) and Cisco TelePresence Video Communication Server (Cisco VCS).

Cisco TMSPE allows video conferencing network administrators to create and manage mass-deployable video conferencing solutions. This is done by using the following features:

- Importing user accounts in bulk from external directories such as Active Directory followed by scheduled or on-demand synchronization.
- Organizing users into a group hierarchy to allow for differences in configuration requirements such as available bandwidth, available endpoint device types, or access rights to phone books.
- Specifying configuration templates and address patterns that are applied to all users in a group.
- Distributing the provisioned settings and phone books to users through Cisco TelePresence Video Communication Server.
- Deploying FindMe™ with the end-user FindMe portal residing on the Cisco TMS server and accessed using AD login. This feature allows users to specify which video and audio devices should ring when someone calls their ID.

This deployment guide

This guide covers the deployment and maintenance of Cisco TMSPE with Cisco TMS version 14.1.

Users of previous versions of Cisco TMS must refer to the deployment guide for their version.

This document provides best practices and step-by-step instructions for installing Cisco TMSPE to the Cisco TMS server.

The document also describes typical maintenance tasks for Cisco TMSPE administrators, and a troubleshooting section is included.

Provisioning builds upon existing capabilities in Cisco TMS and Cisco VCS, and this guide assumes familiarity with both products. We recommend that only technically trained users perform the procedures described in this document.

Release notes

We recommend reading the software release notes for both Cisco TMSPE, Cisco TMS, and Cisco VCS software for detail on initial installations or upgrading.

Prerequisites and recommendations

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

Cisco TMS and server requirements

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

Product	Version and description
Cisco TMS	■ Version 14.2. Users of earlier versions of Cisco TMS must refer to the deployment guide for their version. ■ See hardware recommendations below. ■ For complete Cisco TMS requirements, see *Cisco TelePresence Management Suite Installation Guide*. Note that trial versions of Cisco TMS cannot activate this extension.
SQL Server connection	■ 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	■ 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 : • Windows Server 2003: http://support.microsoft.com/kb/958687 • Windows Server 2008 R2: http://support.microsoft.com/kb/2194664 and http://support.microsoft.com/kb/2194664 Note that the default connection protocol is TCP/IP. If this protocol is used, no hotfixes are required.
Cisco TMS Provisioning Extension option key	■ 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	Cisco TMSPE has been tested with Java 7, update 40 and update 17, 32-bit and 64-bit versions. (For Windows Server 2003, only 32-bit Java is supported.) Download the installer from www.java.com. **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.

Hardware recommendations

For optimal performance, we recommend the following hardware specifications depending on the size of your deployment and user base:

- Small deployment: 4 GB RAM, 2 GHz dual-core processor
- Medium deployment: 4 GB RAM, 2 GHz quad-core processor
- Large deployment: 8 GB RAM, 2 GHz quad-core processor

Cisco TelePresence Management Server

Cisco TMSPE may be installed on the now discontinued Cisco TelePresence Management Server, but note that system resources are limited to 2 GB RAM, which will reduce performance. We recommend using the server for small deployments only and ultimately migrating to hardware with more resources available.

No support for multiple network cards

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

Cisco VCS requirements

VCS Control must be version X7.2 or later. Option keys must be added for:

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

SMTP server requirements

A valid SMTP server that will accept SMTP relay from the Cisco TMS server is required to send account information to users from Cisco TMSPE. If your SMTP server requires authentication, make sure this information is available during configuration.

Database Server Requirements

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.

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 TMS. When prompted for SQL Server credentials during installation, enter the username and password for that account. Cisco TMSPE will create the tmspe database automatically using the server defaults, assign itself as the owner and continue to use the supplied account to access the database after installation.
- Manual database creation, max security limited role. Ask your SQL server administrator to create:
  - A database named tmspe with the appropriate options. The database collation must be Latin1 General CI (case insensitive) and AI (accent insensitive). (Latin1_General_CI_AI).
  - An SQL user and login to use for the Cisco TMSPE Service account and grant the user the dbowner role for the database.

Note: When using the manual database creation, ensure that database settings **ALLOW_SNAPSHOT_ISOLATION** and **READ_COMMITTED_SNAPSHOT** are set to *On*.

Note: For Cisco TMSPE to function properly, the SQL user supplied must always have dbowner permission on the tmspe database, even after installation.

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	▪ *sysadmin* if the installer will create the database on the MS SQL server ▪ *db_owner* if using a manually created database on the MS SQL server. See Manually creating the database on the MS SQL server [p.9] for further details.

For operation

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

Application	User Privilege
Cisco TMS SQL server instance	*db_owner*
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.

Manually creating the database on the MS SQL server

If the Cisco TMS **tmsng** database is located on an external SQL server, the database administrator must do the following prior to installation:

- Create an empty database **tmspe** in the same instance as **tmsng**.
- Apply collation `Latin1_General_CI_AS`.
- Create a user with the *db_owner* role for use during installation of Cisco TMSPE. The same user will be utilized for operations.

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 its SQL db (**tmspe**) to the same location and instance. 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** database to another location and instance. However, we recommend storing the **tmspe** database in the same location as the **tmsng** database. Note that the database name must be **tmspe** in lowercase.

CAUTION: Installing with a new, manually created database does not work with Cisco TMSPE 1.1. You must let the Cisco TMSPE installer create the database for you, or, if manual creation is required, install Cisco TMSPE 1.0 first and then upgrade to 1.1.

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 Required security permissions [p.9] section for appropriate operation permissions.

WebEx Enabled TelePresence requirements

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

- A WebEx Enabled TelePresence option key.
- One or more WebEx sites.
- Single sign-on or specified WebEx credentials for each user (not service user).

For guidance on setting up WebEx Enabled TelePresence, see *WebEx Enabled TelePresence 2.0 Configuration Guide for Cisco TelePresence Management Suite*.

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

Smart Scheduler and FindMe have been tested with the following browsers and versions:

- Microsoft Internet Explorer 10 and 9
- Firefox 15 and 16
- Google Chrome 24
- Safari for Mac OS X 6.0.2
- Safari for iPad 6.1.1

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

Best practices for deployment

Upgrade endpoints to the latest software

Prior to installation and deployment of Cisco TMSPE, we recommend upgrading all endpoints to the latest software version available.

This ensures that the configuration template schemas are compatible with Cisco TMSPE and limits the number of templates and schemas to maintain post-installation.

At the time of Cisco TMSPE 1.0 release, endpoint software version recommendations are as follows:

Software	Version
Cisco Jabber Video for TelePresence	4.2 or later
Cisco IP Video Phone E20	TE4.1.1 or later
Cisco TelePresence System EX and MX Series	TC5.1 or later

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 provides the option of enabling HTTPS communication. We strongly recommend enabling HTTPS and using valid certificates. Cisco TMS will otherwise offer to create a self-signed certificate.

Make sure the encryption settings match the available certificates when configuring Cisco VCS communication, see Setting up communication between Cisco TMS and Cisco VCS [p.22].

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*.

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 [p.75].

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

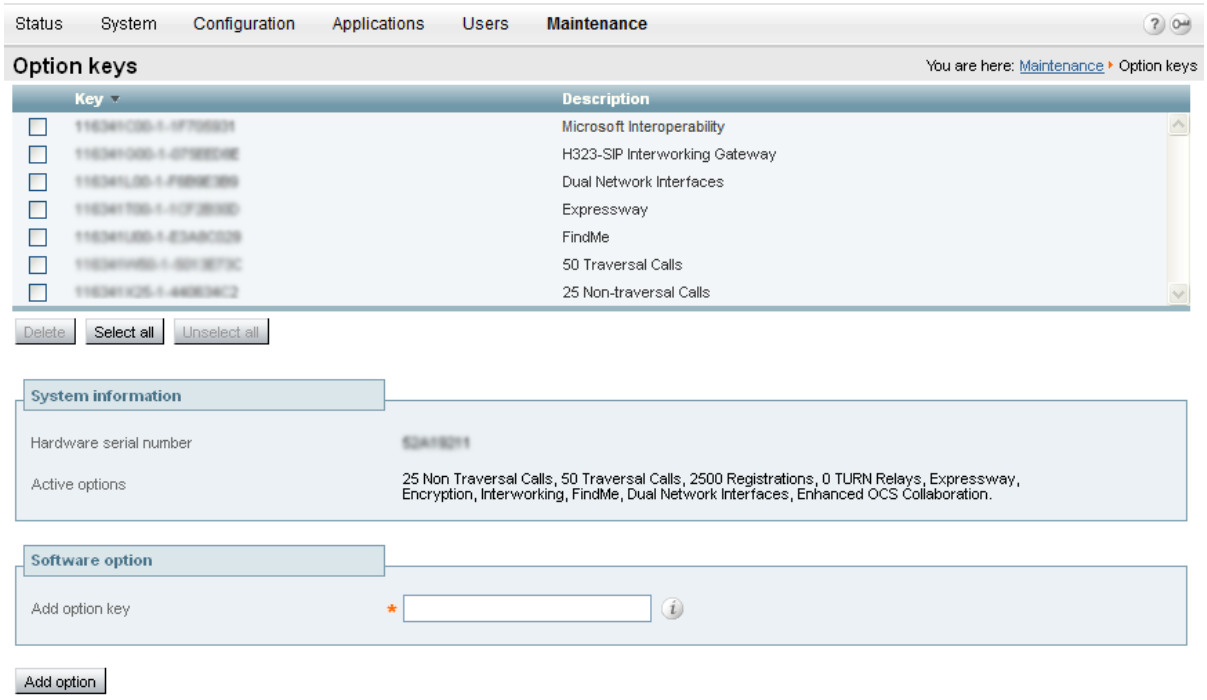
Installing the Device Provisioning option key

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 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**.



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**).

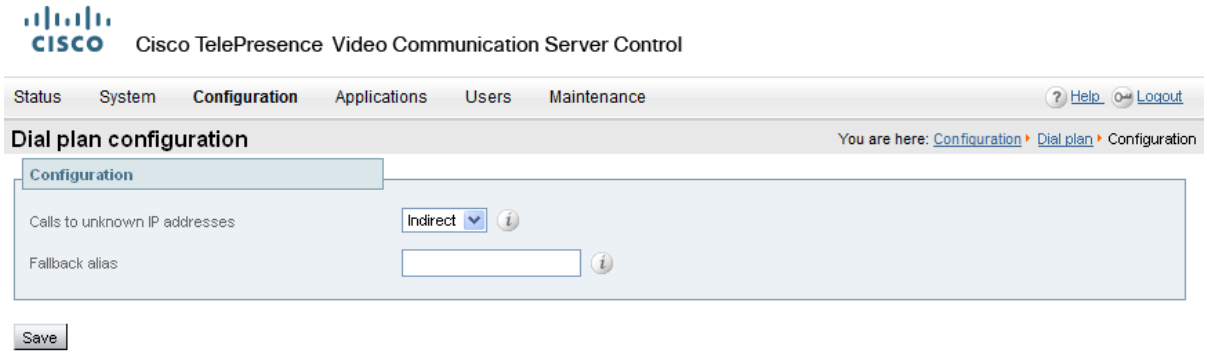
Configuring how Cisco VCS handles calls to unknown IP addresses

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**).

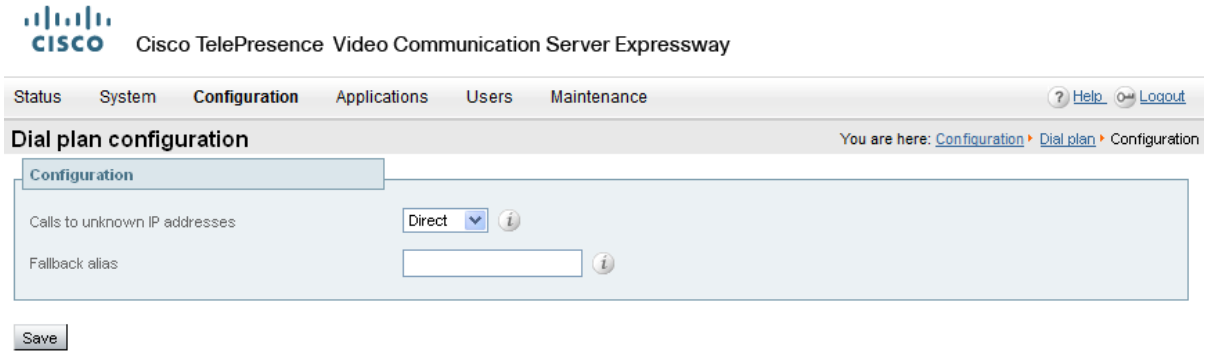
VCS Control

Set the VCS Control to use the *Indirect* mode for **Calls to unknown IP addresses**.



VCS Expressway

If you are using a VCS Expressway, it must be set to use the *Direct* mode for **Calls to unknown IP addresses**.



Adding the Cisco VCS to Cisco TMS

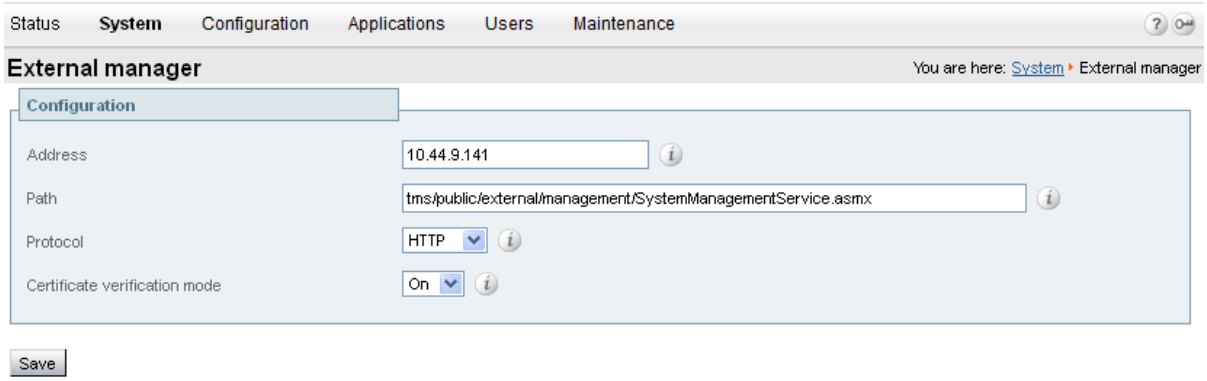
This procedure is compulsory for the Cisco VCS (or Cisco VCS cluster) on which provisioning is enabled (typically the VCS Control), and optional for other Cisco VCSs (a VCS Expressway, for example).

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 an **SNMP community name** is set.

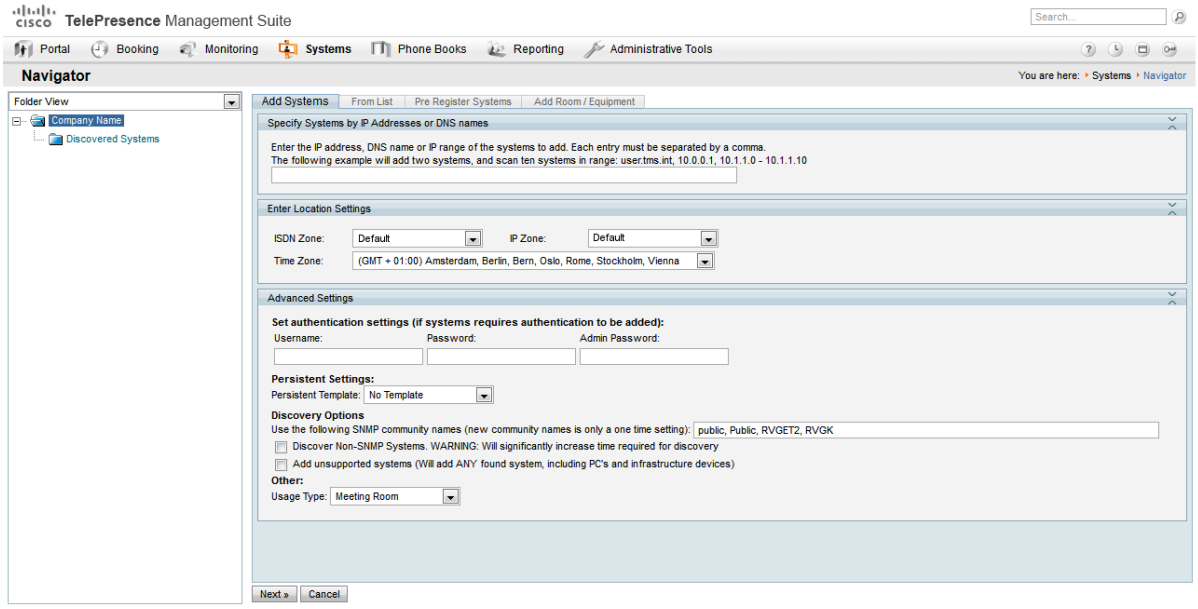
- If SNMP is not permitted inside your network, you can add VCS Control to Cisco TMS without SNMP. However, this will negatively impact Cisco TMS's ability to auto-discover and monitor the Cisco VCS.

2. Ensure that the IP address or FQDN of the Cisco TMS is set up in **System > External manager > Address**.



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. If SNMP mode is *On* in the Cisco VCS, enter the VCS IP Address and click **Next**. Cisco TMS will collect information from the VCS about how best to communicate with it.
   - If you do not support SNMP on your network, the VCS can be discovered using alternative means in Cisco TMS. See the section for discovering non-SNMP devices in *Cisco TMS Management Suite Administrator Guide*.
4. Click the **Add Systems** button in the right pane. Follow the instructions in Cisco TMS to add the Cisco VCS.



5. Ensure that the Host Name of the Cisco VCS is set up in Cisco TMS:
   a. Go to **Systems > Navigator**.
   b. Select the VCS.

c. Select the **Connection** tab.

6. Set **Host Name** to be the FQDN of the Cisco VCS, for example vcs1.example.com.
7. Click **Save/Try**.

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

When using FindMe, 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**.

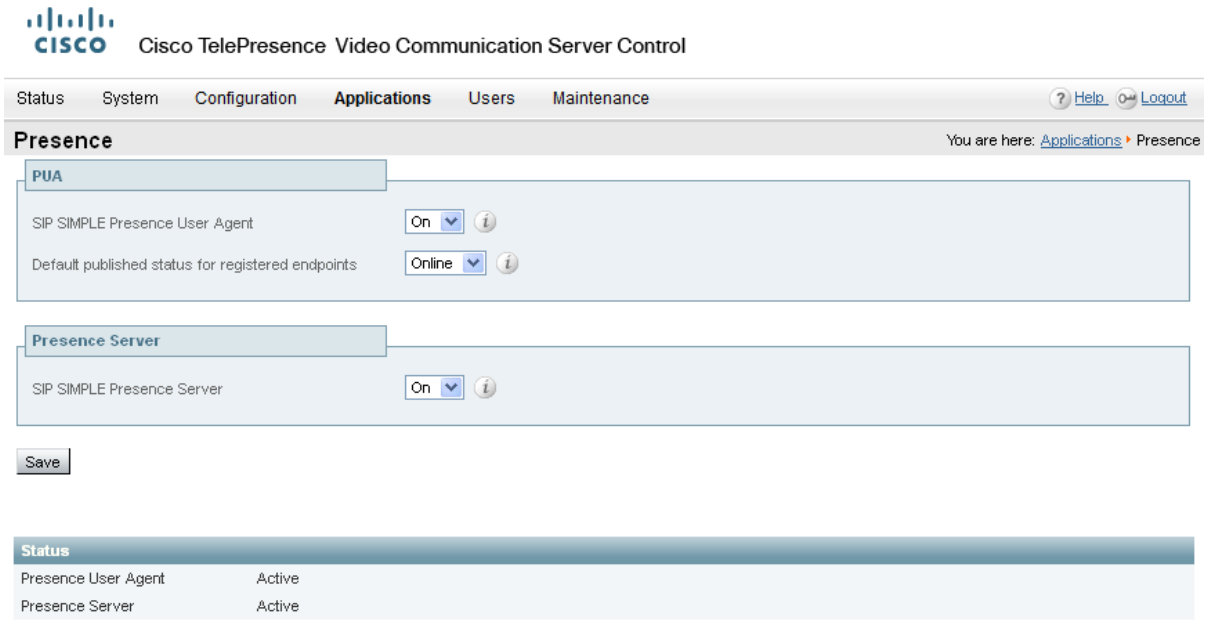
Enabling Presence on the Cisco VCS

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.

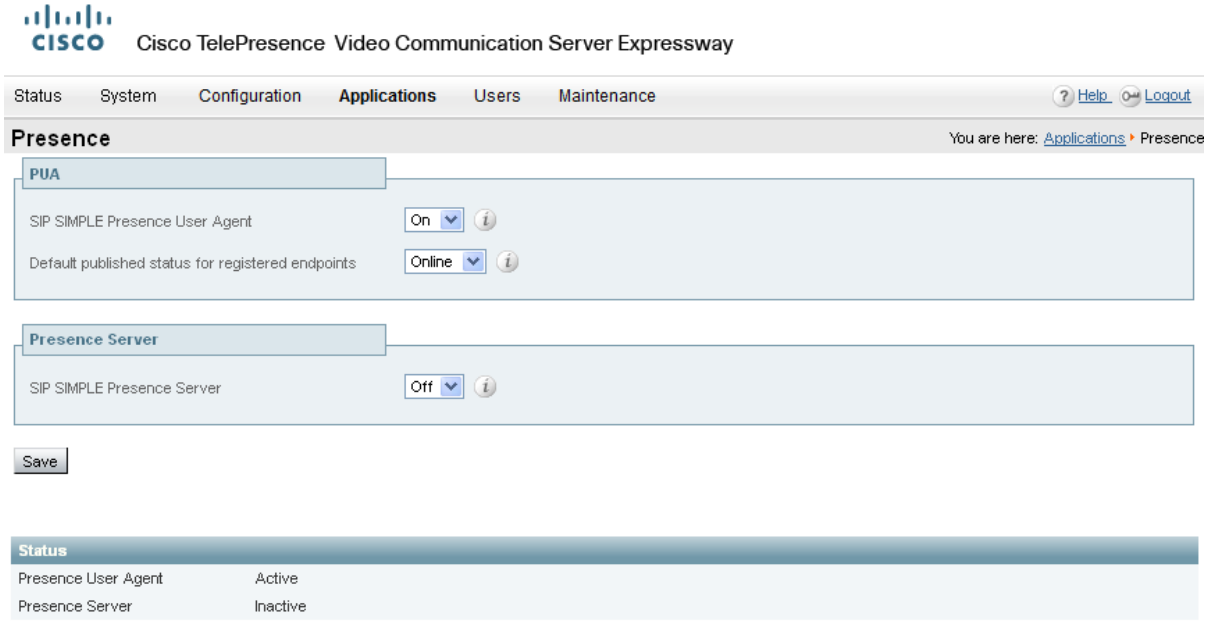
Presence on VCS Control

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*.



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*.



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. To verify:
  - If using Cisco VCS X7.1, go to **Configuration > Zones** and select the **Default Zone**.
  - If using Cisco VCS X7.2 or later, go to **Configuration > Zones > Zones** and select the **Default Zone**.
- Any traversal client zones:
  - If using Cisco VCS X7.1, go to **Configuration > Zones**, then select each zone of type *Traversal client*.
  - If using Cisco VCS X7.2 or later, go to **Configuration > Zones > Zones**, then select each zone of type *Traversal client*.
- The Default Subzone. These settings are found at **Configuration > Local Zone > Default Subzone**.
- Any other configured subzones. Go to **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 [p.20].
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.21].

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 Administrator Guide*.

Upgrading from previous versions

To upgrade from Cisco TMSPE 1.0:

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.
5. Follow the installer instructions.

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

To configure the new Smart Scheduler for use, see Deploying Smart Scheduler [p.42].

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.
5. Follow the setup instructions:
   a. Click **Next** to initiate the setup.
   b. Accept the terms in the license agreement and click **Next**.

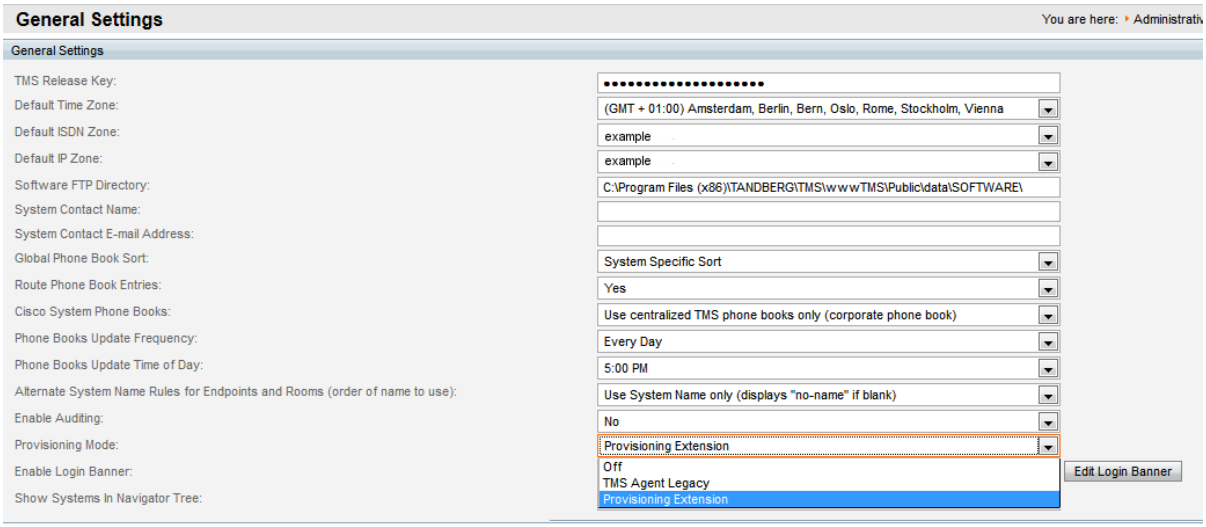
c. Enter the **Username** and **Password** of the service user that Cisco TMSPE will use to connect to Cisco TMS. This user must be a member of the Site Administrators group in Cisco TMS. Click **Next**.
d. The installer detects where the TMS SQL database (`tmsng`) is installed. We recommend installing the Cisco TMSPE SQL database (`tmspe`) to the same location and instance.
   i. Confirm or enter the appropriate **SQL Server Name** and **Instance Name**. 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**.
e. Click **Install** to begin the installation. Click **Back** to review or change installation settings.
f. 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.



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 [p.70].
      - **Systems > Provisioning > FindMe**
      - **Systems > Provisioning > Devices**
      - **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.70] 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 [p.22].

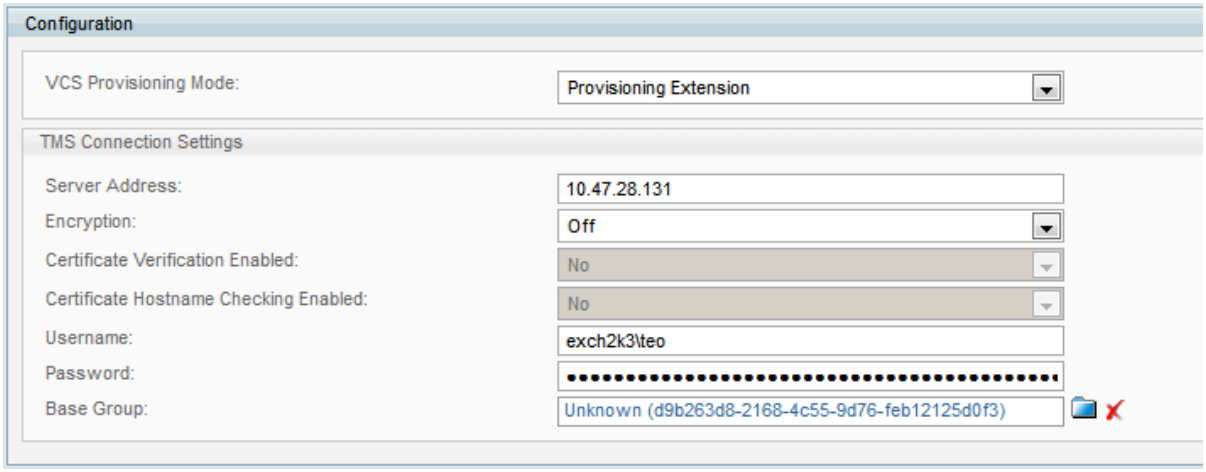
Setting up communication between Cisco TMS and Cisco VCS

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.

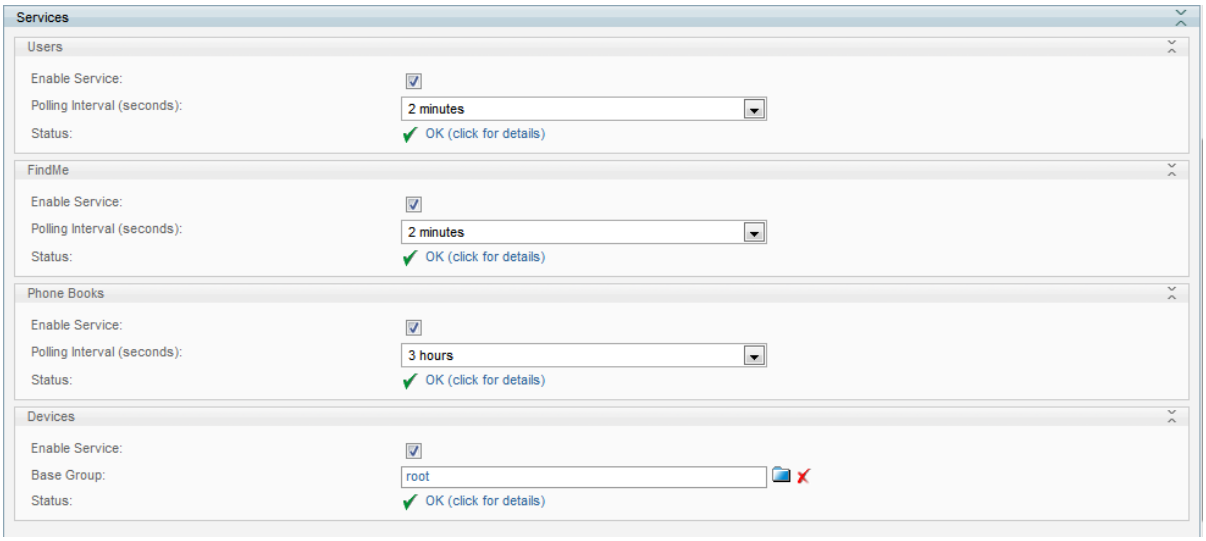
- Cisco VCS imports the user configurations, FindMe settings, phone books and licensing information from Cisco TMSPE.
- Cisco TMSPE receives information about provisioned devices from Cisco VCS.

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 default and recommended **Encryption** setting is *TLS*, see Use secure communication [p.12]. 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**.



8. When green check marks are displayed for all services, scroll to the **VCS Provisioning Mode** field at the top of the page and select *Provisioning Extension*. Click **Save**.

You can now proceed to Setting up users and provisioning [p.24].

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 potential 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 the user, FindMe, phone book, and device 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

You can import and synchronize user account data from the following external sources:

- Active Directory
- Active Directory with Kerberos
- Lightweight Directory Access Protocol (LDAP)

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

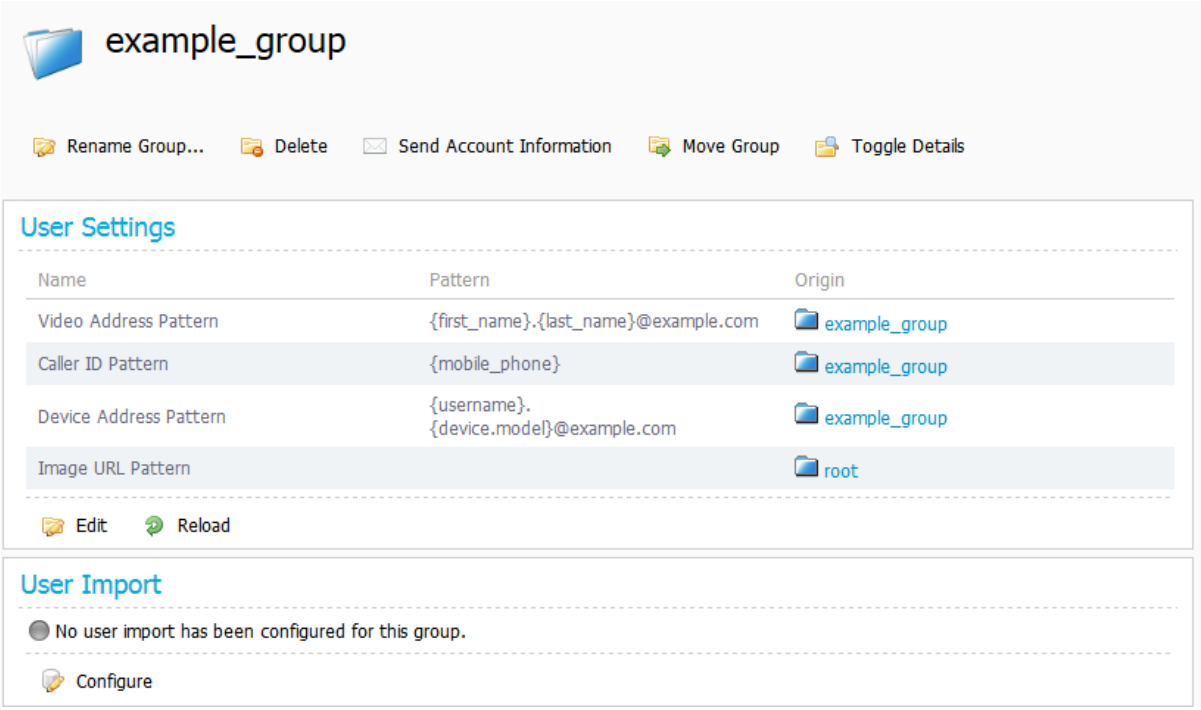
- An **`entryUUID`** field as defined by RFC 4530.
- Simple paging as defined by RFC 2696.

Imports are set up per group. Before you configure an import, 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.

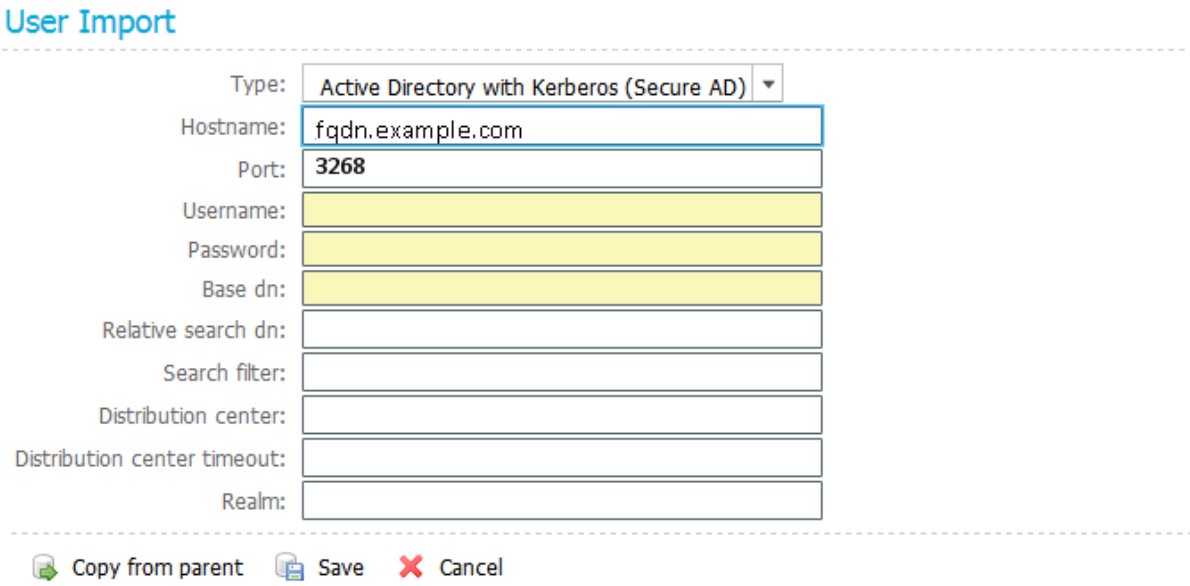
Setting up an import

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.



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:



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 `C:\example\folder\myfile.txt`, the relative DN is `myfile.txt`. 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: • *Unsecured* • *StartTLS* • *SSL*— note that no certificate handling is supported for this connection type.
Ignore certification errors	No	No	Yes	Select *Yes* or *No*.

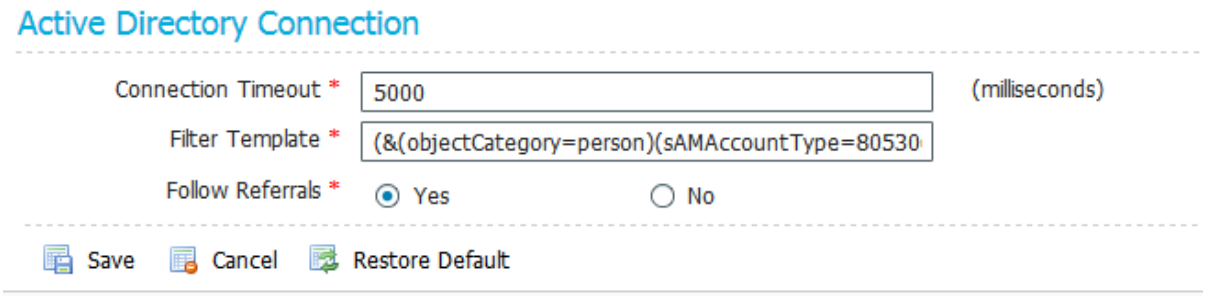
7. Click **Save**.

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.62].

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.



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.27].

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**.

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 number.

Additionally:

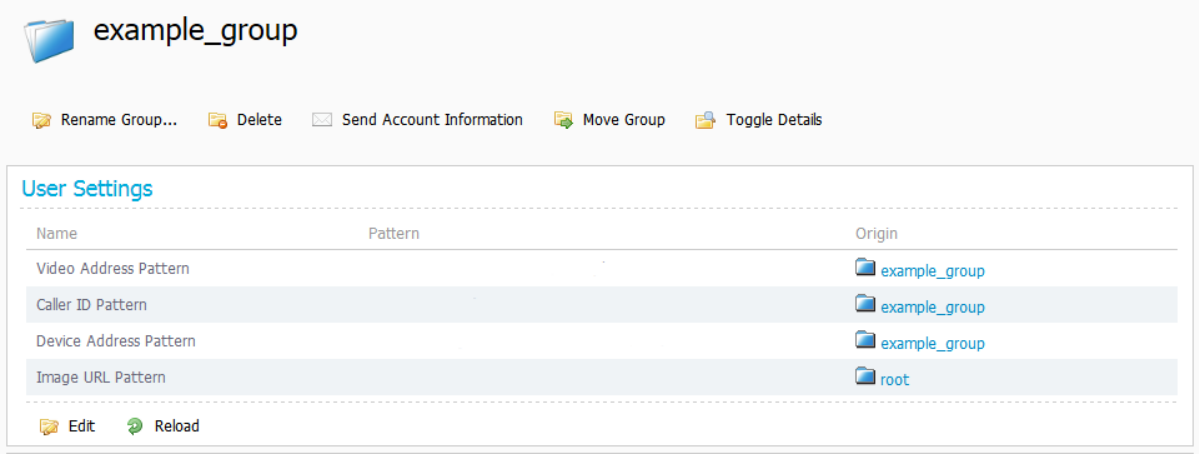
- The **Caller ID pattern** is used by FindMe to generate caller IDs for calls routed through an ISDN gateway. Defining caller ID patterns [p.46] is described in the Deploying FindMe [p.46] section of this document.
- An **Image URL pattern** may optionally be added when configuring user groups, if a 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.

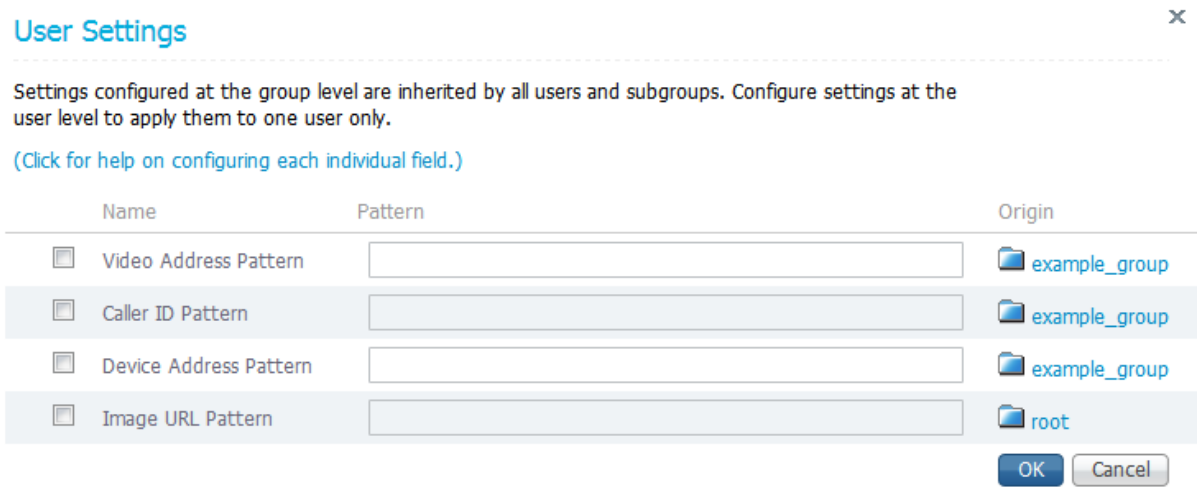
Adding the patterns

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

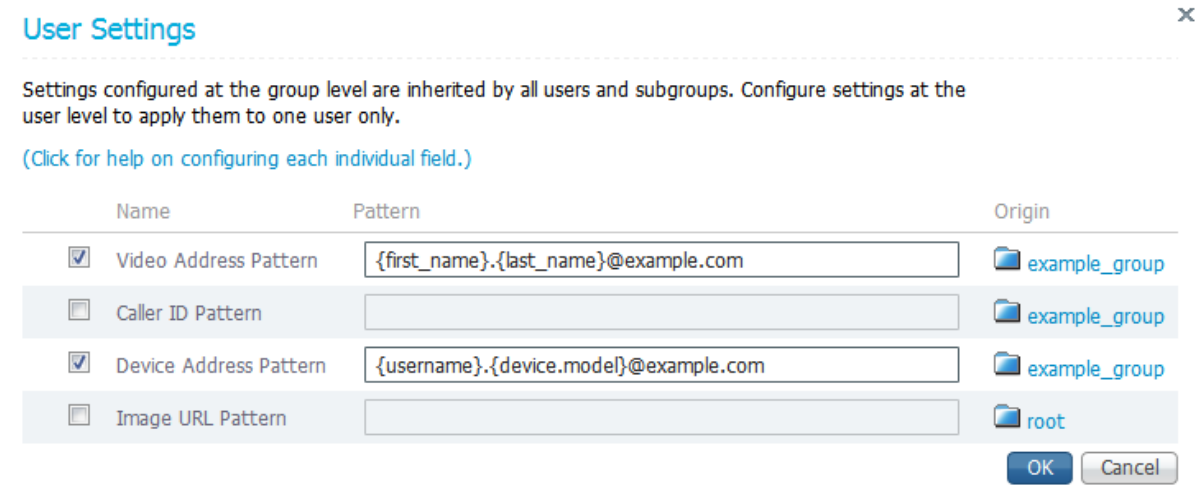
1. In Cisco TMS, go to **Systems > Provisioning > Users**.
2. In the **Users and Groups** container, navigate to and click the group to which you want to assign a device address pattern.



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



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.



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`**

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'.

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

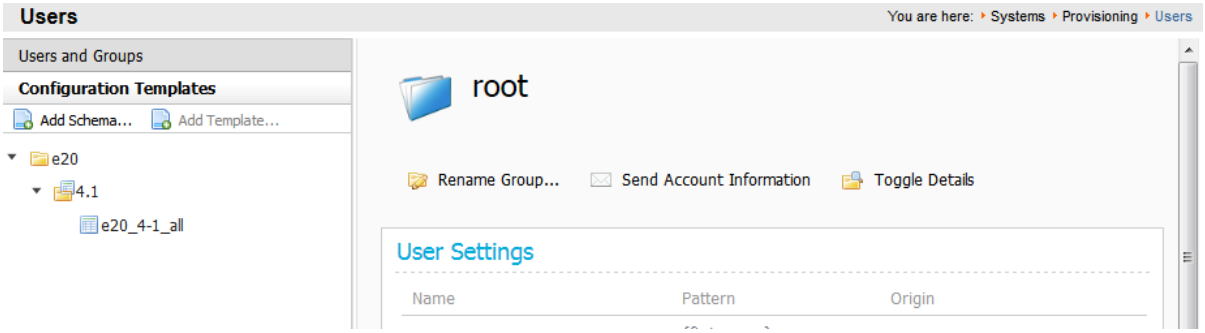
For each model and version of endpoint available on your network, you must obtain the relevant schema and upload it to Cisco TMSPE. Template schemas are usually included with device software releases, either inside the software bundle, or on the same page as the release notes are made available. If the 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:

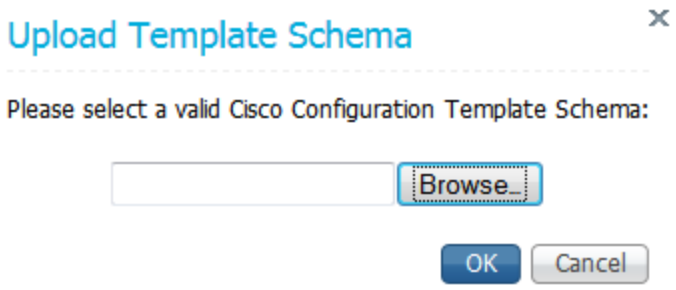
1. Enter "Configuration Templates for TMS" as your search string.
2. Scroll down the list of search results to locate the .zip file containing the required schema.

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.

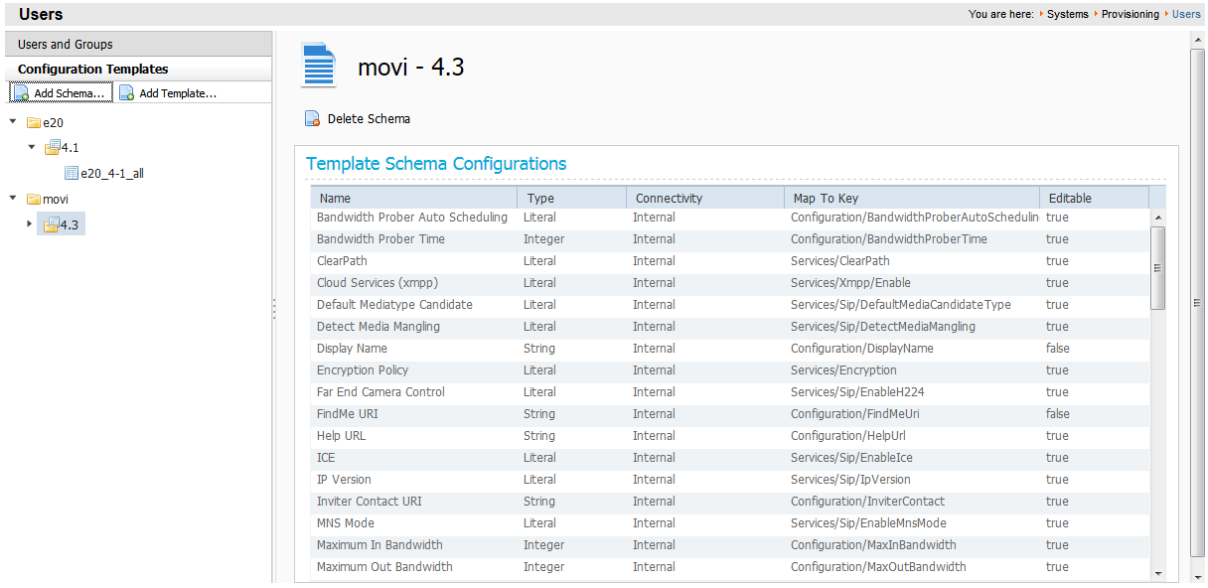


3. In the **Configuration Templates** container, click **Add schema**. The **Upload Template Schema** dialog box opens.



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 [p.30]).

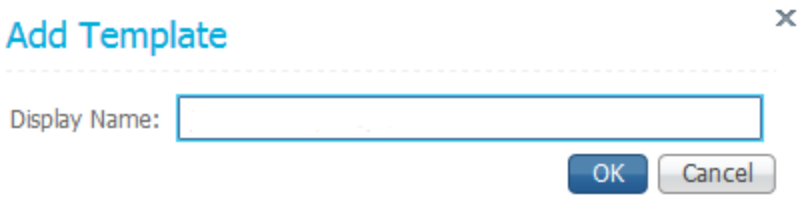
Depending on the types of endpoint devices on your network and the services in use, the following configurations are usually the most important:

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

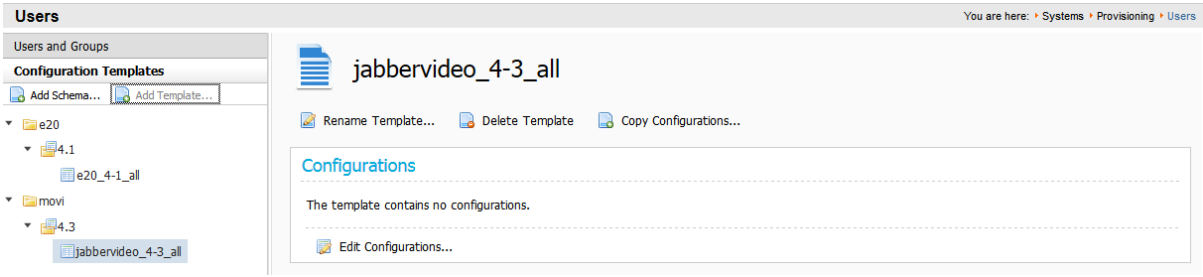
For details on the available configurations and restricted values for each type of endpoint, see the administrator documentation for the endpoint.

To create a configuration template:

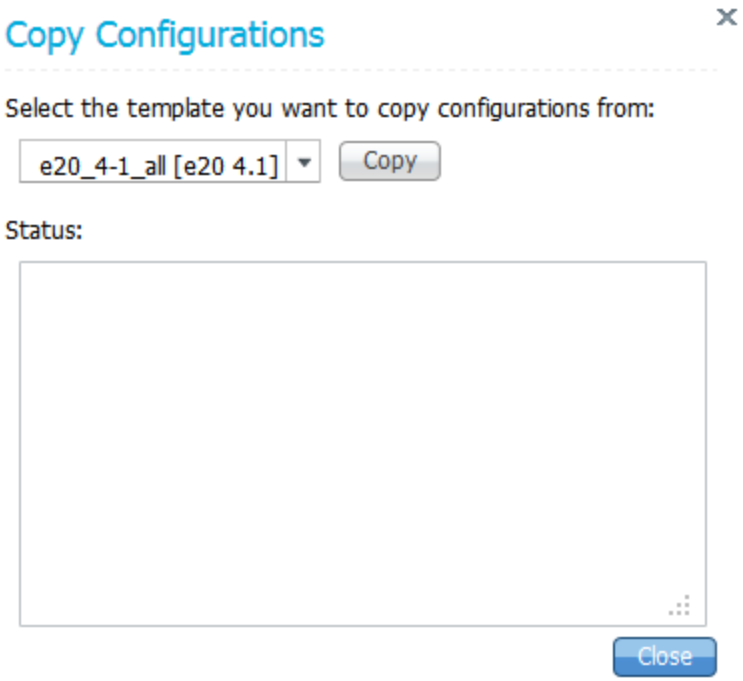
1. On the **Users** page, click the **Configuration Templates** container.
2. In the **Configuration Templates** container, navigate to the folder for the relevant model and version of device, and then click **Add template**. The **Add Template** dialog box opens.



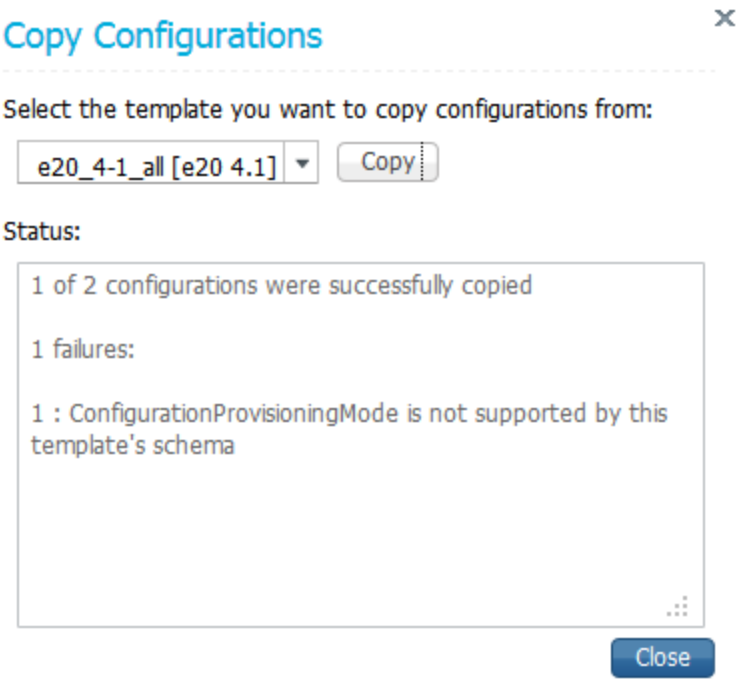
3. Enter a suitable display name for the template, and then click **OK**. The template is added to the **Configuration Templates** container. At this point, the template contains no configurations.



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

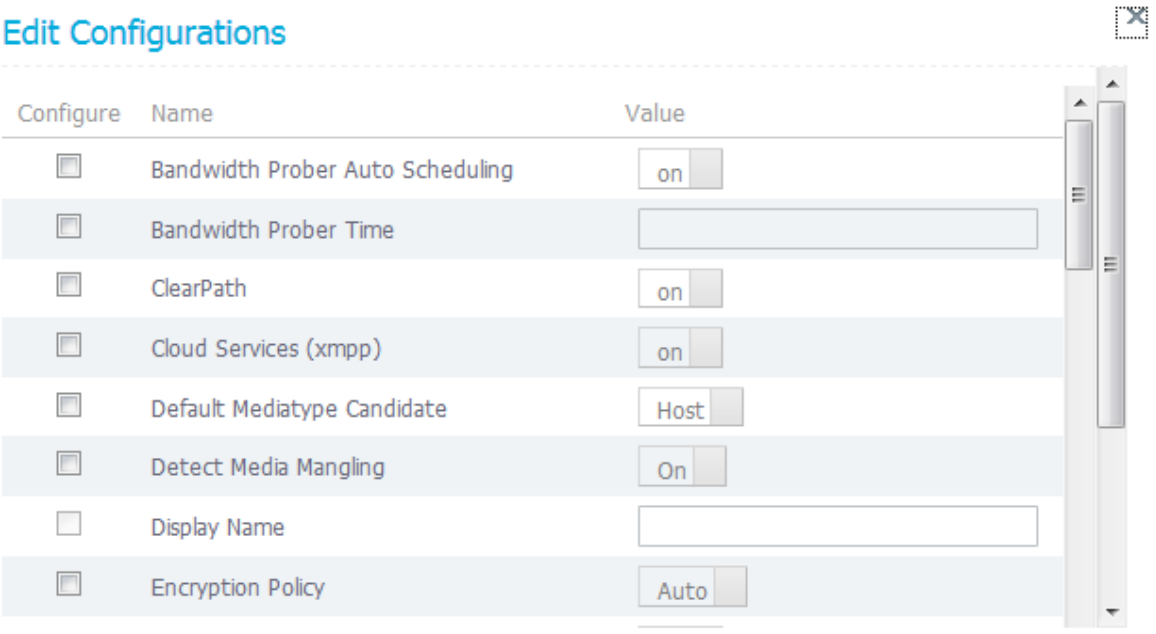


     ii. Select the template from which you want to copy all configurations, and then click **Copy**. The **Status** field reports the result of the copy. The number of successfully copied configurations is displayed, as well as the number that failed to copy, for example, due to the target template's schema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



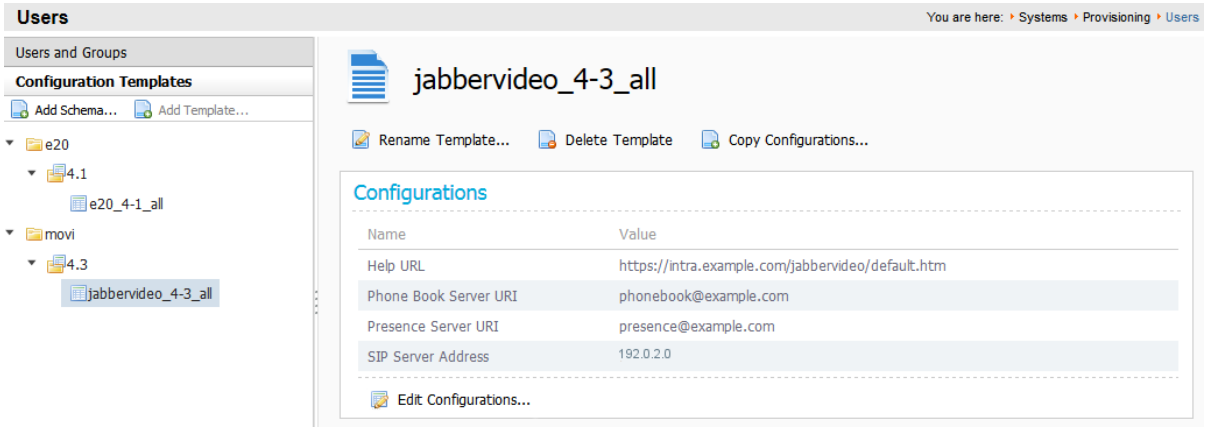
iii. Click **Close**.

- Add individual configurations:
  i. In the **Configurations** pane, click **Edit configurations**. The **Edit Configurations** dialog box opens.



  ii. 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.
  iii. 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.

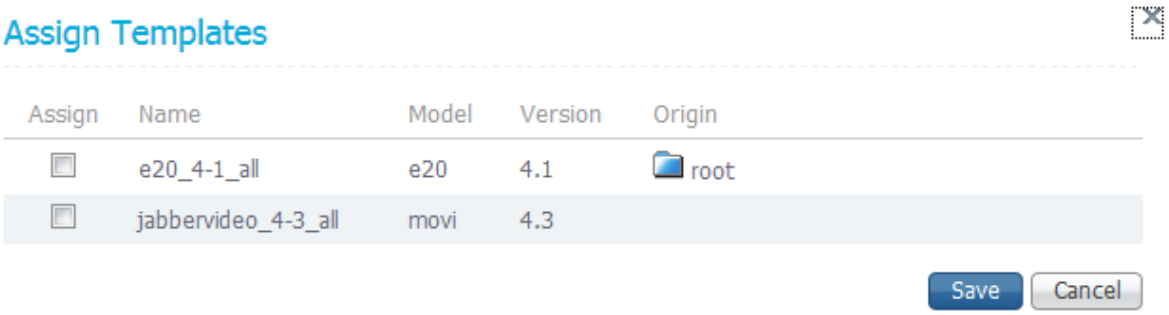
Assigning configuration templates to groups

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.

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

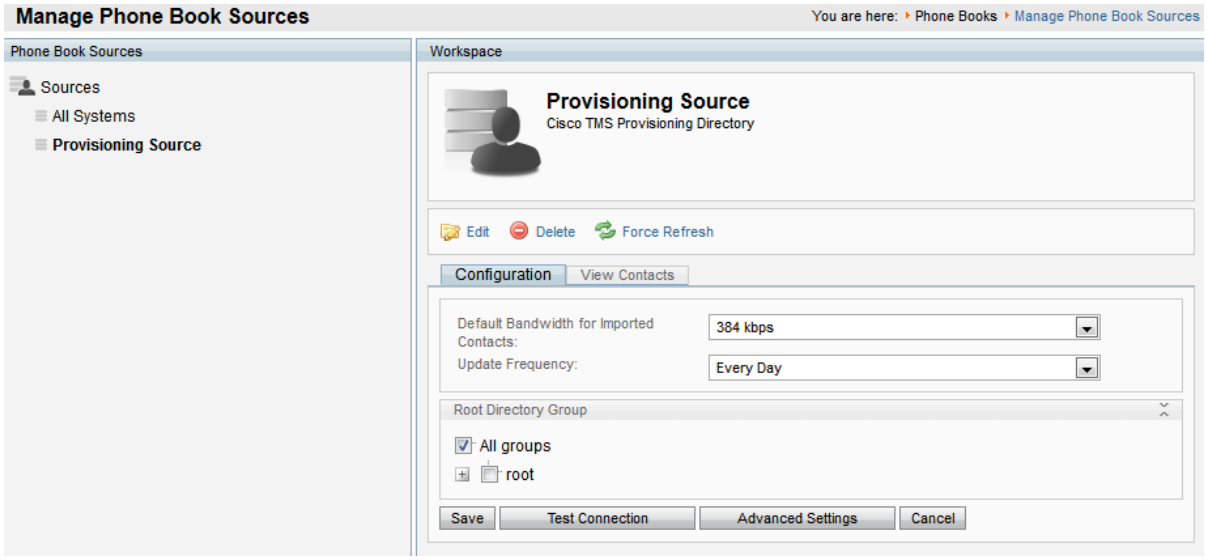


3. Select the check box for each configuration template that you want to assign to the group.
4. Click **Save**.

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



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 > Provisioning Source**.
2. Click the **Advanced Settings** button to open settings that configure what is included in the source .
   - Check **Provisioned Devices** to have device addresses added to the source as users log in and devices are provisioned.
   - Check **Office Phone** and **Mobile Phone** to include these fields for imported or manually created provisioning users.

3. In the **Root Directory** 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:

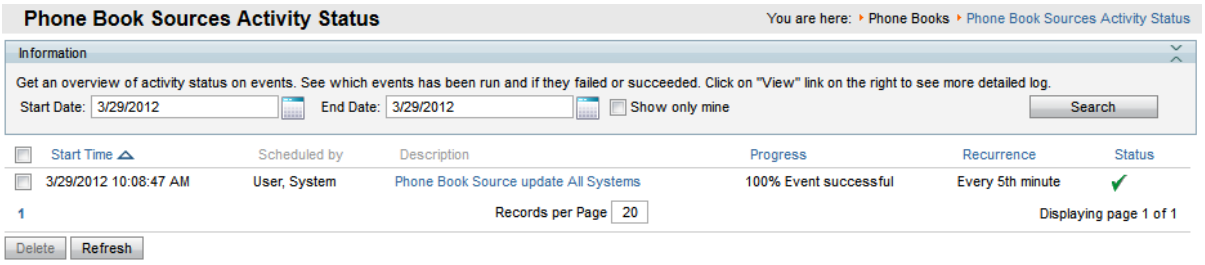
1. Go to **Phone Books > Manage Phone Books**.
2. Click **New**.
3. Enter a display name for the phone book and click **Save**.

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.



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.

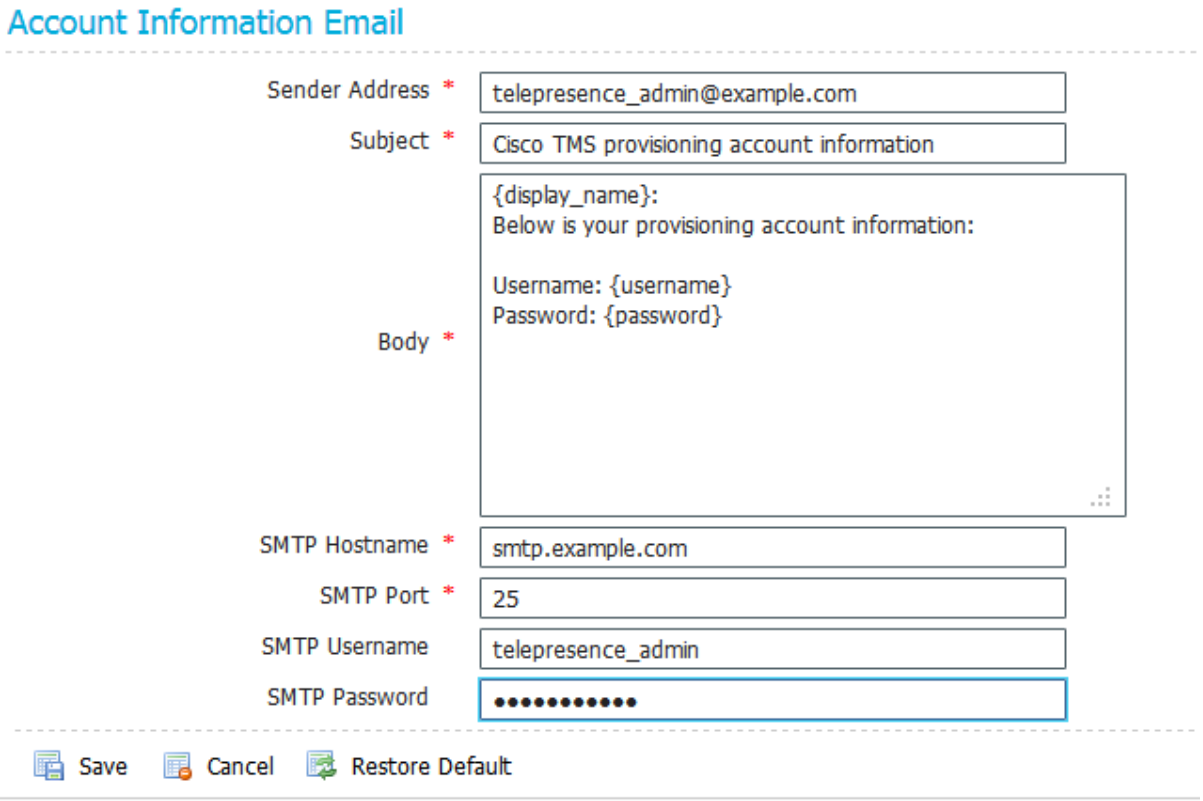
Configuring and sending account information

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**.



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	Template that determines the body of the email sent to users. For an example, see the screenshot above. If using FindMe, we recommend adding the following additional information: `You can be contacted via your FindMe ID: {video_address}.`
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*.

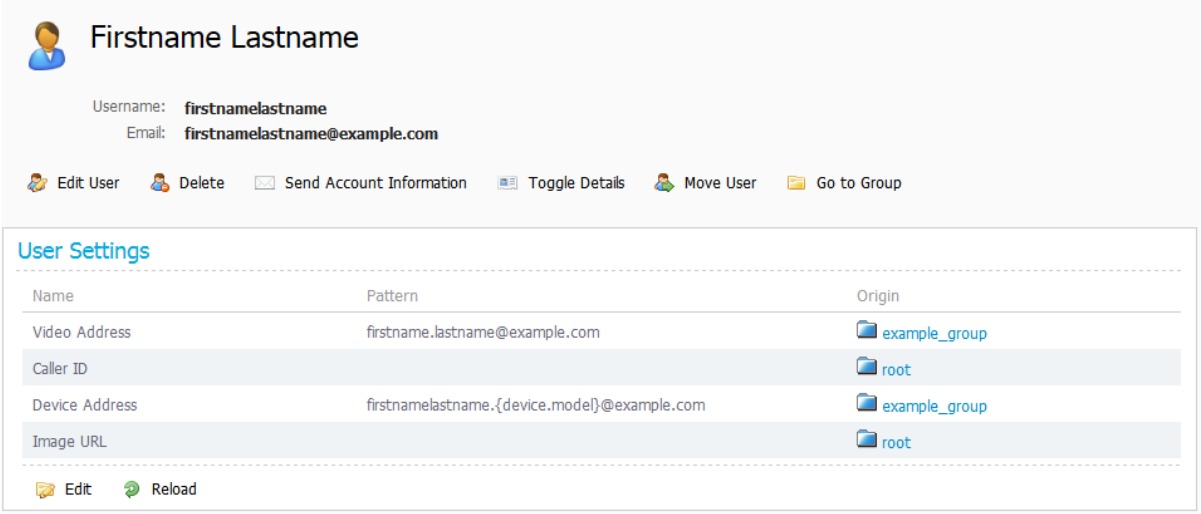
4. Click **Save**.

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, 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.



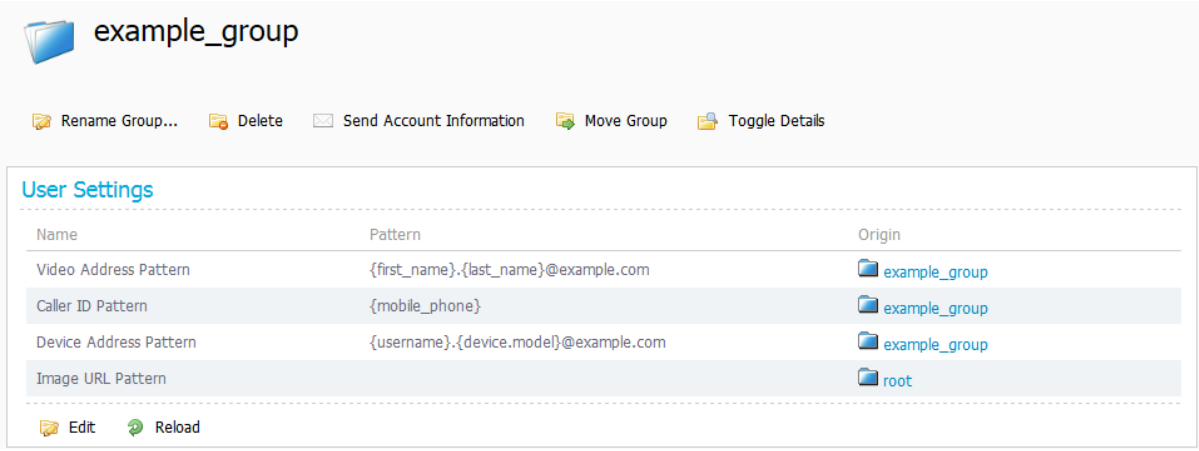
3. In the area above the **User Settings** pane, click **Send Account Information**.
   A message is displayed confirming that the email has been scheduled for sending.
   Depending on the configuration of your email server, the scheduled email should arrive in the selected recipient's inbox within a few minutes. If the email fails to be delivered, check the **Alarms** pane on the **Diagnostics** page. See Running Cisco TMSPE diagnostics [p.68].

Sending account information to all users in a group

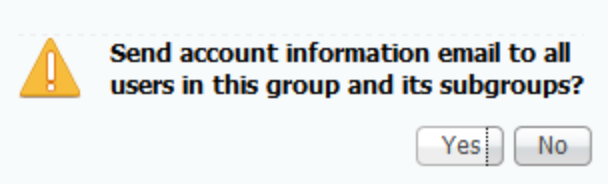
When you select a group to notify, Cisco TMSPE notifies all users in that group as well as users in all subgroups.

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.



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



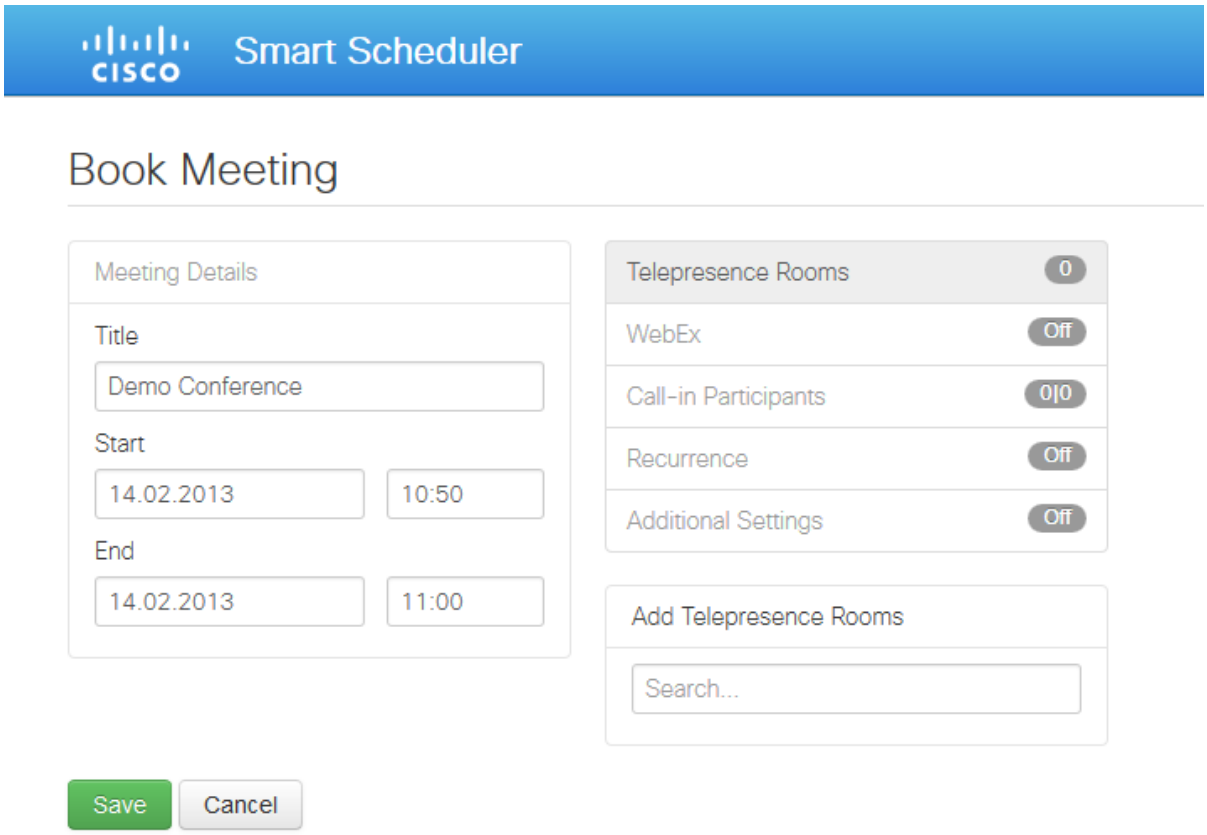
4. Confirm that you want to send account information to all users in the group. A message is displayed confirming that the email has been scheduled for sending. If the email fails to be delivered, check the **Alarms** pane on the **Diagnostics** page. See Running Cisco TMSPE diagnostics [p.68].

To send account information to any additional users added at a later date, if automatic sending of email to imported users is not enabled, notify the users individually as explained in Sending account information to a single user [p.40]

Deploying Smart Scheduler

Smart Scheduler is a smart, clean interface to Cisco TMS booking, using the Cisco TelePresence Management Suite Extension Booking API (Cisco TMSBA). It uses the same portal framework as the FindMe user portal.

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.

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 instances.
- Smart Scheduler will rename call-in participants added from Cisco TMS.

Booking limitations

Booking through Cisco TelePresence Management Suite Extension Booking API has the following limitations:

- The use of setup and teardown buffers in Cisco TMS is not supported.
- 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 default 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.
- You cannot move a meeting from the past to the future. This includes changing the start time of a meeting that is already ongoing.

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 modifying a recurrent series while an occurrence is ongoing:

- changing the start time will be applied to the entire series, and the ongoing meeting will be disrupted. Meetings set to connect automatically will be reconnected.
- any other modifications will be applied to upcoming instances only, and the ongoing meeting will be marked as an exception in Cisco TMS.

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 will therefore be the same for all users.

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 Smart Scheduler. 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.

Note that if a user configures a time for their computer that is different from their time zone, bookings will still be created based on the time zone information rather than the configured computer time.

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.9].

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 [p.24]. 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 [p.28]. 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 number.

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 [p.60].

Defining caller ID patterns

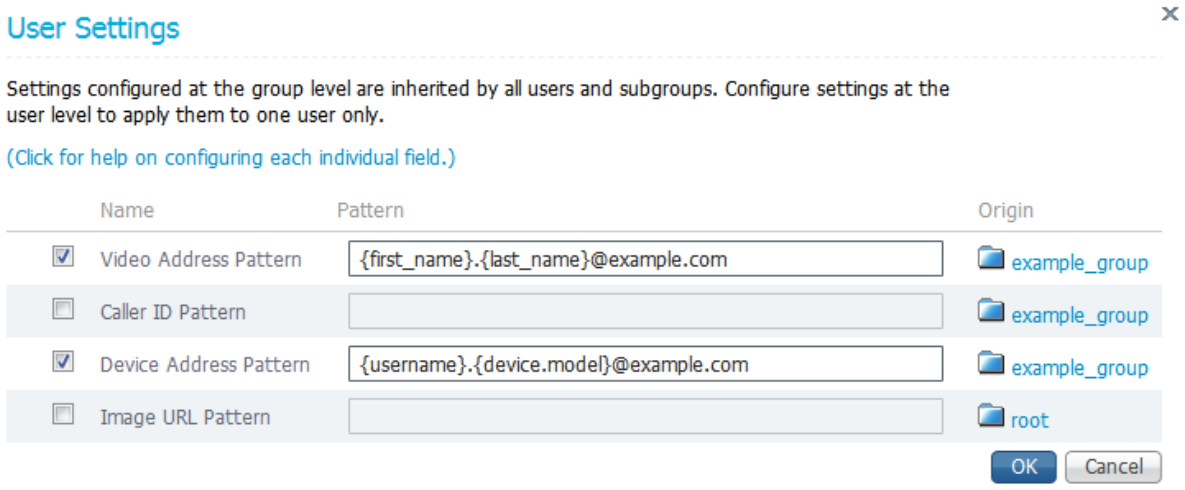
Caller ID patterns are used to generate each user's callback number, which is used when a FindMe call is routed through an ISDN gateway. This ensures that a user who is contacted on their phone will see a number that they are able to call back, rather than a video address, even if the person calling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

Assigning a caller ID pattern to imported accounts

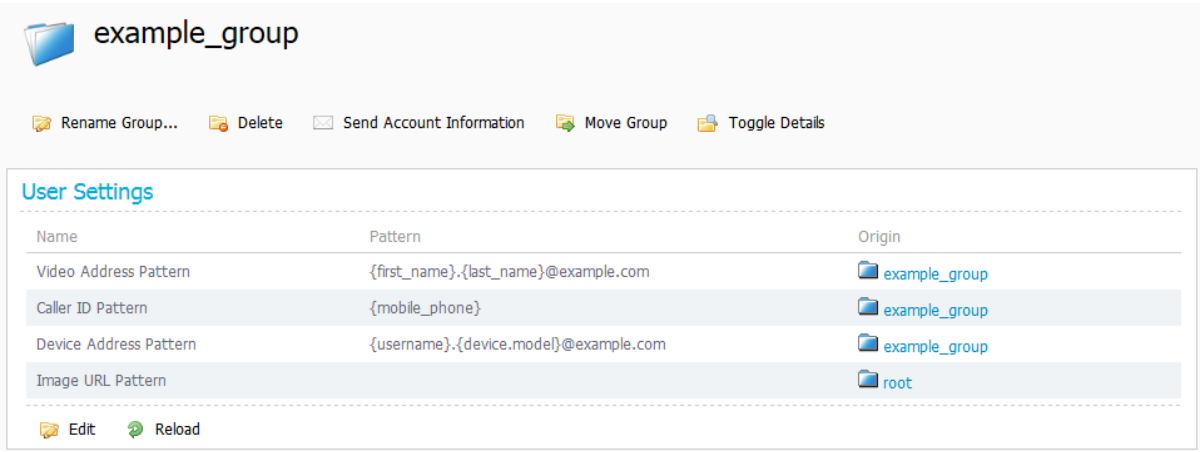
This procedure applies only to FindMe accounts that are imported from the **Users** page. For manually created FindMe accounts, define the FindMe ID and caller ID while creating or editing the accounts—see Manually adding FindMe accounts and groups [p.48].

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



4. 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}
5. Click **OK**.



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

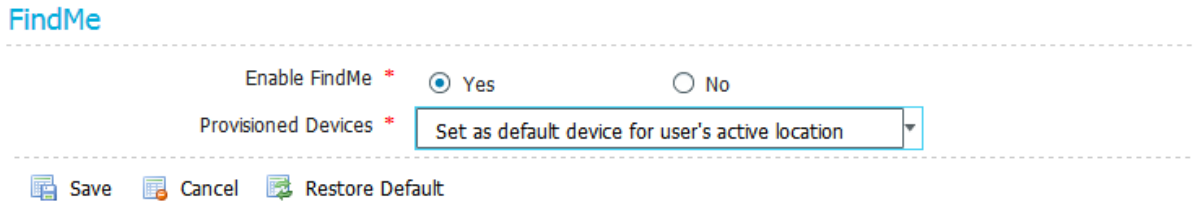
When you enable FindMe in Cisco TMSPE, provisioning users will be imported to the FindMe account view. Before enabling FindMe, make sure to define a video address pattern for all groups and users you want to include in FindMe:

- 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 [p.28] 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.



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:

Set as default device for user's active location	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.
Add to user's device list	When a device is provisioned, add it to the list of devices in the provisioned user's FindMe account.
Do not include	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 [p.69]. 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 [p.60].

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 *Individual* or *Group*.

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 [p.50]
2. Adding FindMe location templates [p.51]
3. Associating device templates with location templates [p.52]
4. Assigning location templates to groups [p.53]
5. Regenerating FindMe locations and devices [p.57]

Suggested minimum setup

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

1. Enable FindMe with the **Include 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 [p.48].

2. Define one location template, for example, named **`Office`**, and accept the default ring duration of 5 seconds. See Adding FindMe location templates [p.51].
3. Assign the location template to the top-level group in the group hierarchy. See Assigning location templates to groups [p.53].

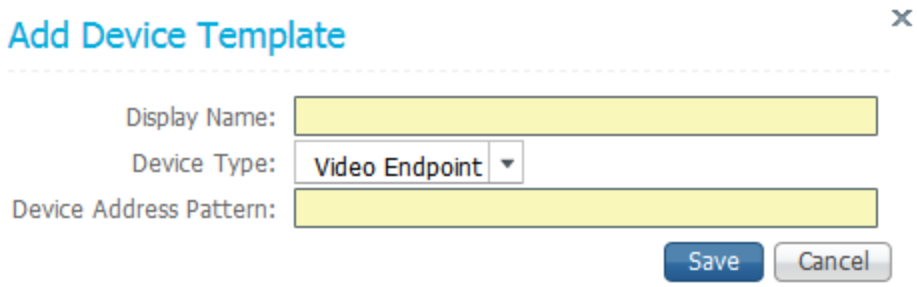
Adding FindMe device templates

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:

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



3. Configure the fields as follows:

Display Name	The FindMe device name; for example, `E20`.
Device Type	The picture to display. Select from the following: • Video Endpoint • Telephone • Mobile Phone • Laptop • Person • Voice Mail. 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. • Video Mail • Group
Device Address Pattern	The pattern to use to create the device address or number; for example, `{username}.e20@example.com`.

4. 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.

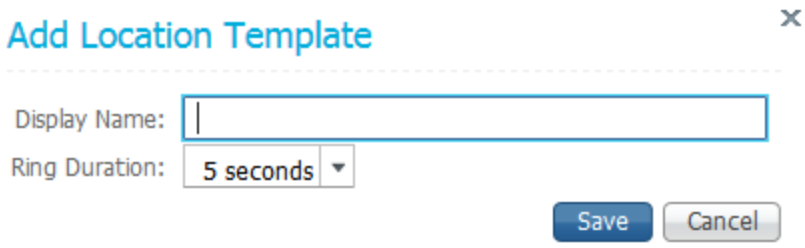
For example, use location templates to represent different physical locations such as "home" or "office", as well as different circumstances such as "on vacation" or "in a meeting".

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.



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

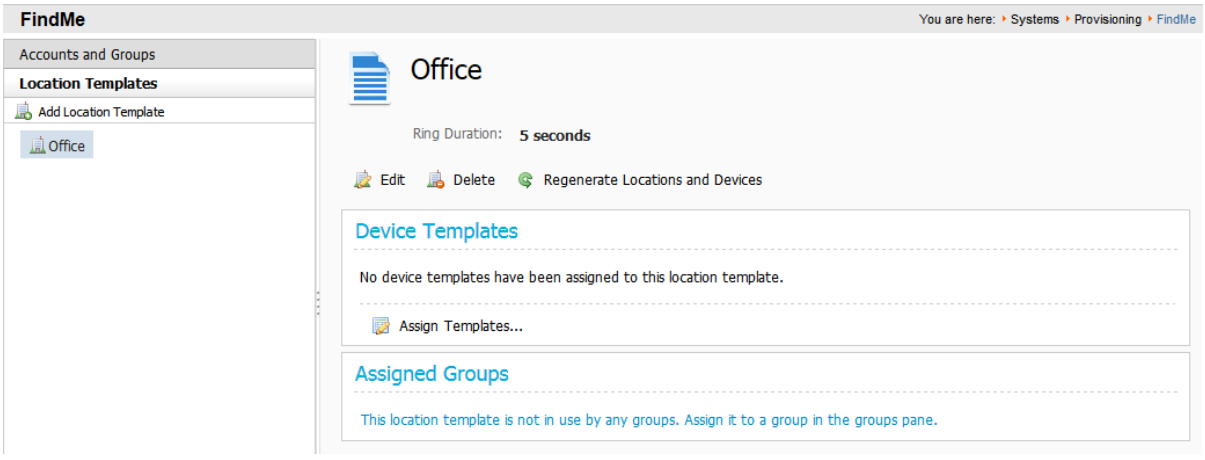
For each location template you add, you must designate at least one device that should be dialed by default whenever a user's FindMe address is contacted.

You can also specify which devices to dial:

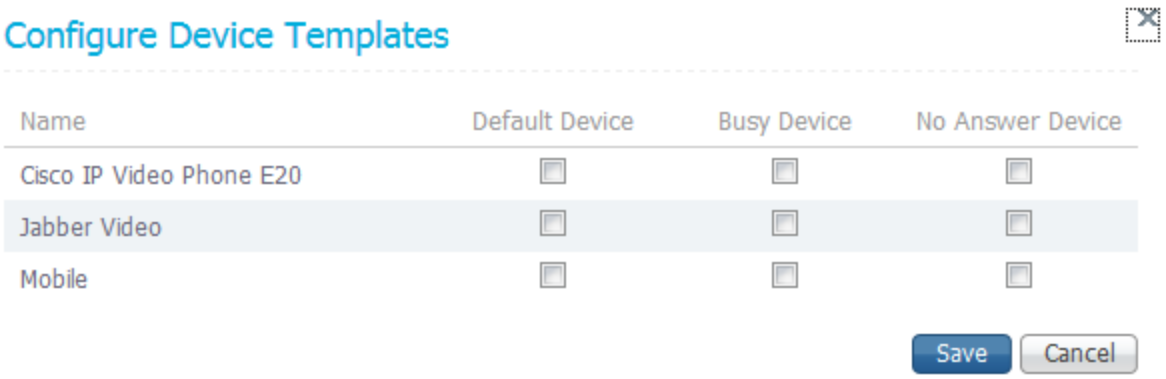
- If the designated default devices are busy.
- If a call is not answered within the location's configured ring duration.

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.

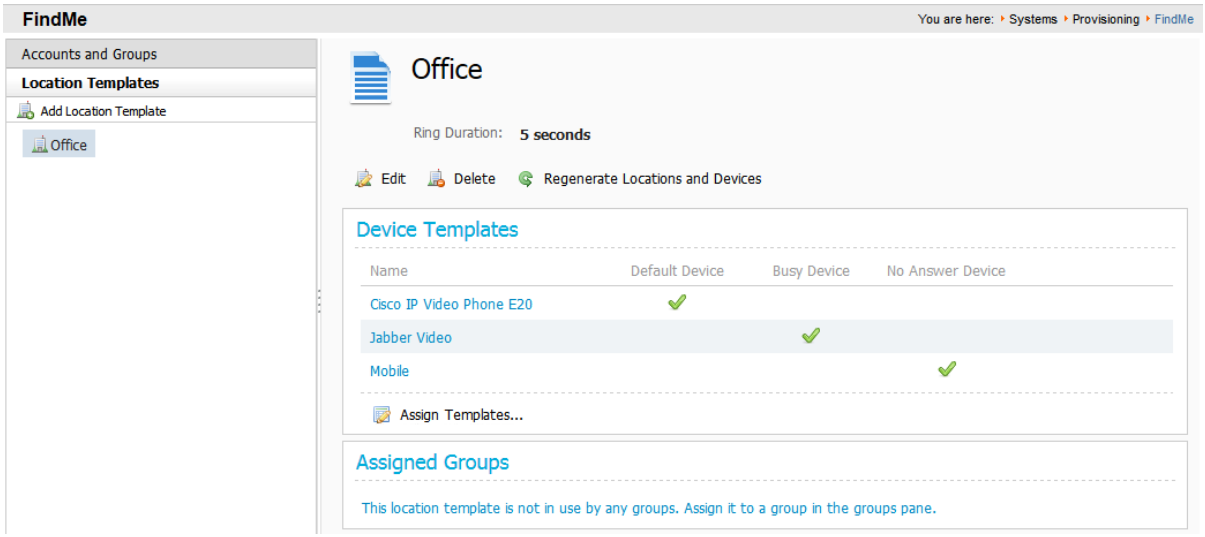


2. In the **Device Templates** pane, click **Assign Templates**. The **Configure Device Templates** dialog box opens.



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**.

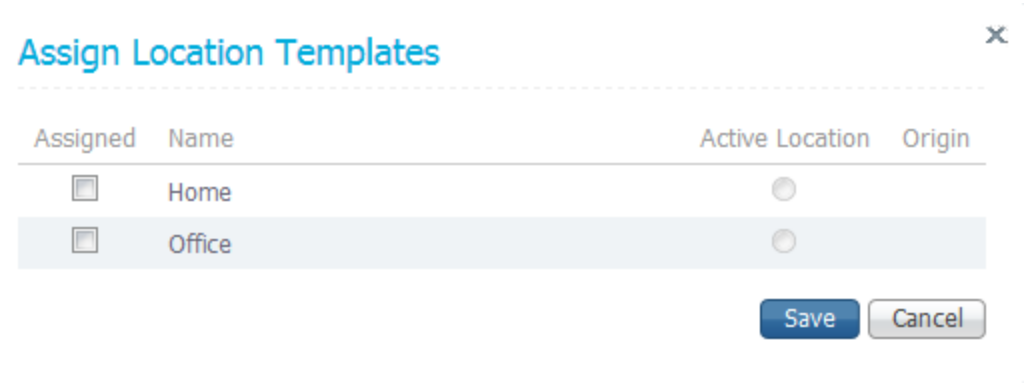


Assigning location templates to groups

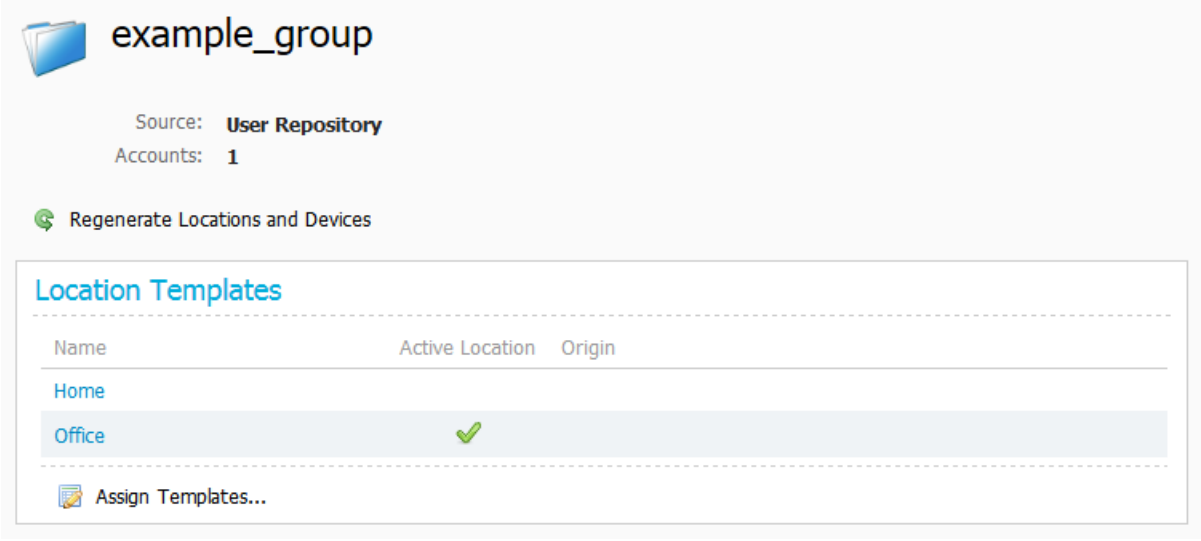
When you assign location templates to a group and apply them by regenerating the group's locations and devices, the information is passed on to and used by the configured VCSs. The location templates also becomes visible to all users in the group the next time they access their user portal. Locations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



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.
6. Click **Save**.



7. Click **Regenerate Locations and Devices...** to apply the templates for all accounts and subgroups in the current group. See Regenerating FindMe locations and devices [p.57] 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 [p.58].

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:

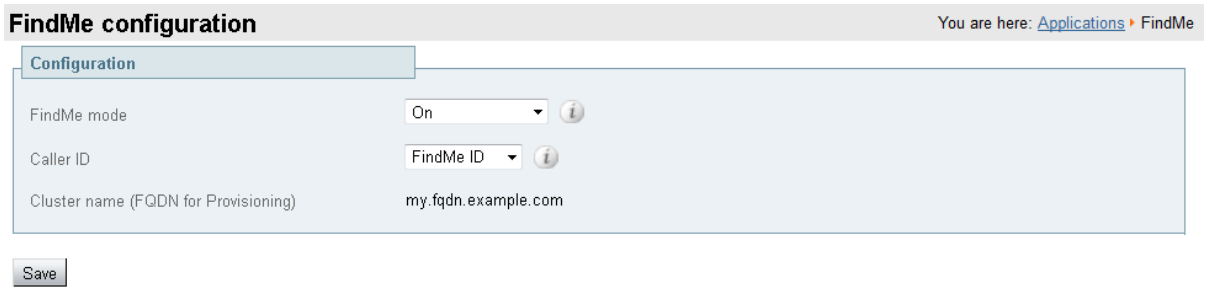
1. Go to **System > Clustering**.
2. Enter the **Cluster name**:
   - If the Cisco VCS is part of a cluster, set it to the fully qualified domain name used in SRV records that address the cluster, for example "cluster1.example.com".
   - If the Cisco VCS is not part of a cluster, set it to the fully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

Enable and configure FindMe settings

To enable and configure FindMe on the Cisco VCS:

1. Go to **Applications > FindMe**.
2. 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 [p.59].
4. Click **Save**.



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 number 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 numbers 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 numbers to FindMe IDs

Using ENUM allows incoming E.164 numbers 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 *not* 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

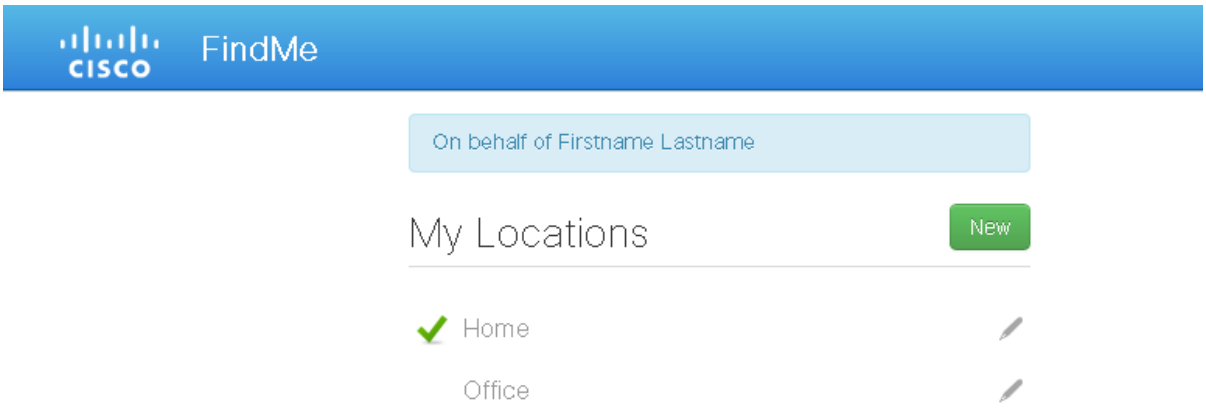
It is not possible to assign location templates directly to single users/accounts. However, if a user needs help or requires a special setup, the administrator can access the FindMe portal on the user's behalf and modify their locations and devices.

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 different 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 [p.24]), 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.63].)

Note that 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.

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:

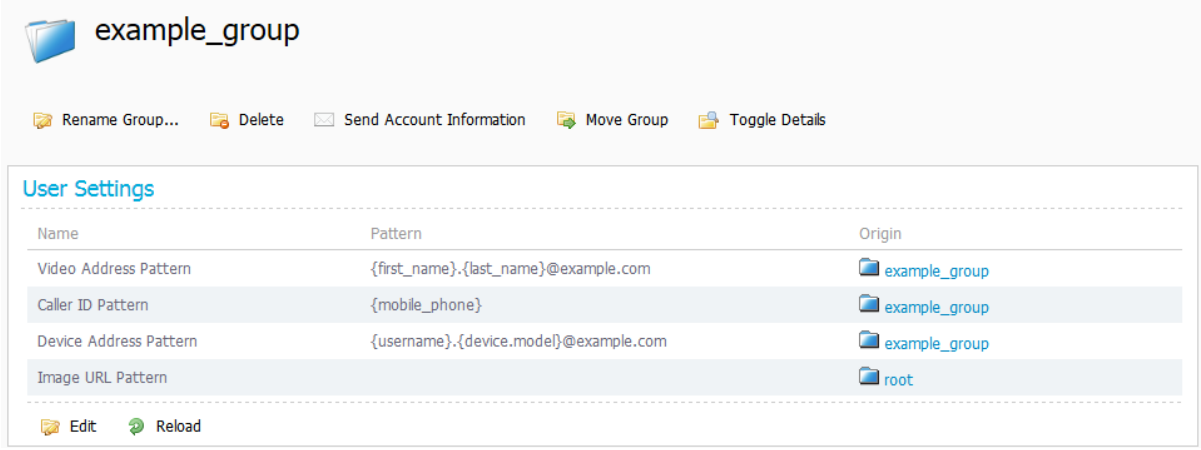
1. In Cisco TMS, go to **Systems > Provisioning > Users**.
2. In the search field below the heading of the **Users and Groups** container, enter the display name of the user account you want to find.
   You can enter a partial search string. User accounts that match the search string are displayed in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

Renaming groups and user accounts

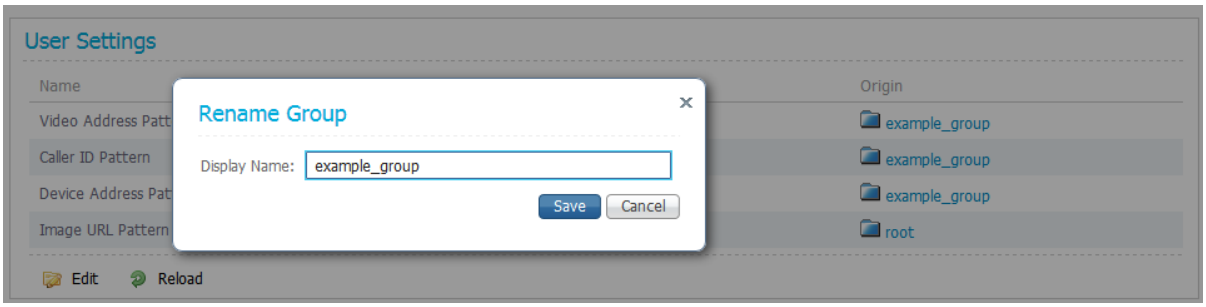
You can change the display name of groups and manually created users.Note that you cannot change the display name of users imported from external directories.

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.



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.

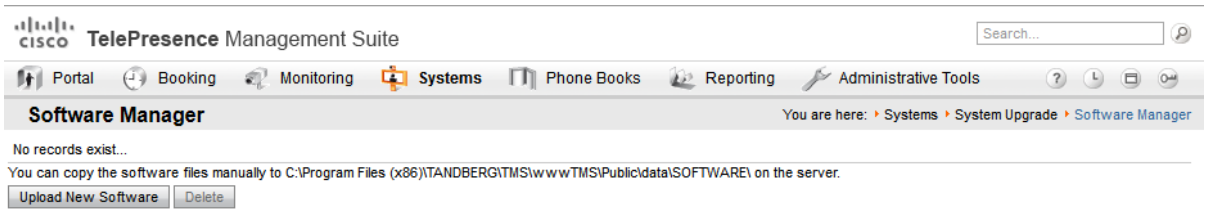
To upgrade configurations:

1. Download and add the new schema. See Obtaining template schemas [p.30].
2. Add a new configuration template based on the new schema:
   a. Copy the configurations from the old template. See Adding configuration templates [p.32].
   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 [p.35].

Upgrading devices

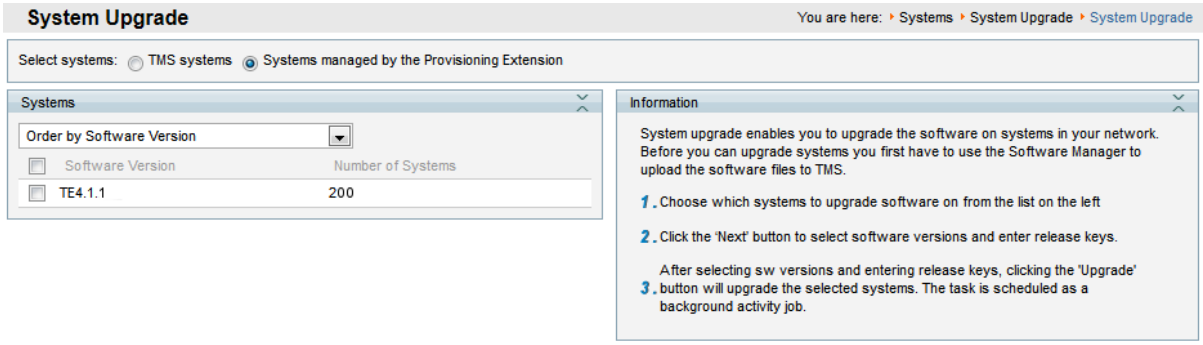
To upgrade hard endpoints:

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.



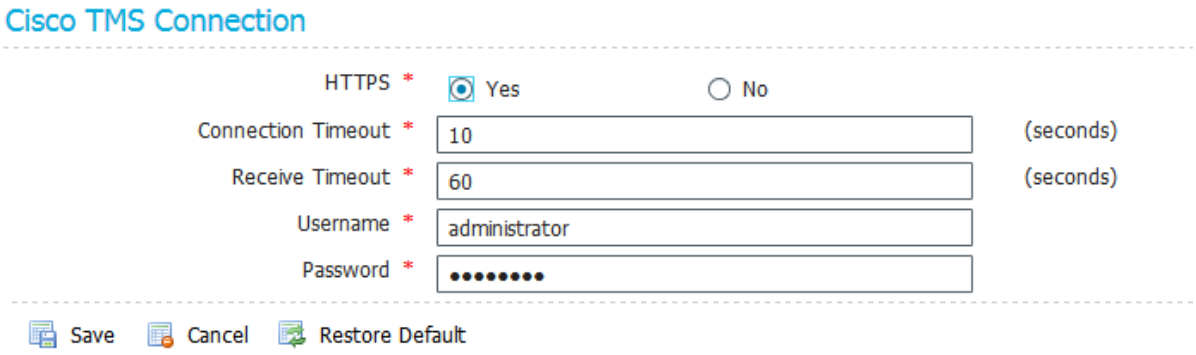
4. Use the options available to select the systems you want to upgrade, and then click **Next**. For information about the options available, see the online help.
5. In the **Release Key** column, enter the release key for each system.
6. From the **Software** column, select the required software package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



3. Modify settings as desired.
4. Click **Save**.
5. Restart the Provisioning Extension service, see Restarting the TMS Provisioning Extension Windows service [p.69].

Maintaining the database

Backing up the database

We recommend backing up the Cisco TMSPE database regularly.

Restoring the database from backup

If restoring the database 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 the database

After moving the database, you must update the database settings in Cisco TMSTools:

1. On the Cisco TMS server, go to **Start > Cisco TelePresence Management Suite > Cisco TMSTools**.
2. Go to **Configuration > Change Provisioning Extension DB Settings**.
3. Update the **Database Server\Instance** with the new location.
4. Verify that the **Database Name** is still **tmspe**.
   Changing the database name is not supported and will break the installation.
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.69] for instructions.

Troubleshooting

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

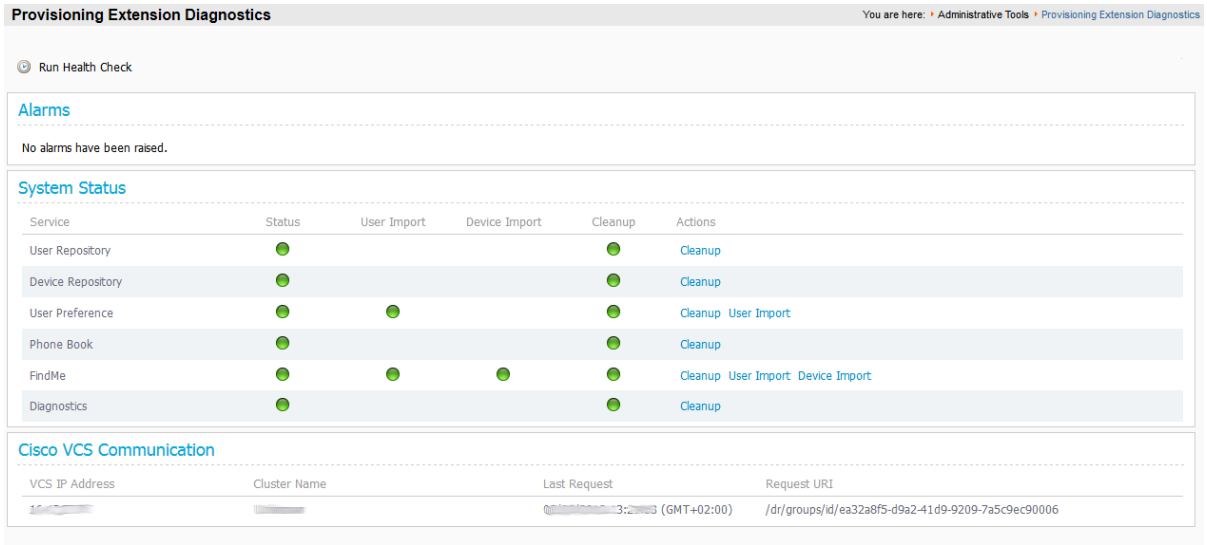
Running Cisco TMSPE diagnostics

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 > 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.



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.

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 2-3 minutes, during which the Cisco TMSPE parts of Cisco TMS will be unavailable.

Provisioning 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\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 TMS and server requirements [p.7].

AD import with Kerberos fails

If you have configured a user import from Active Directory with Kerberos authentication and it fails with an error in the **tmsprovisioningextension.txt** log as indicated below, you are most likely running an unsupported version of Java.

To address the issue:

1. Stop the Provisioning Extension Windows service.
2. Uninstall Java 6.
3. Install Java 7 update 17 (32-bit or 64-bit).
   If changing from a 32-bit to a 64-bit version of Java, you must also re-install Cisco TMSPE.
4. Restart the Windows service.

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.a
pi.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]
```

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 [p.38].
- 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
- 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 [p.30].

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 [p.37].
- 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.

Smart Scheduler and FindMe troubleshooting

Cannot access FindMe or Smart Scheduler

- Error message: Access denied. Verify that all critical Windows Updates are installed on the server.
- If the framework displays a blank page, the user may have manually entered the URL and forgotten the trailing slash.

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\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.69] 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 SQL database `tmspe` when uninstalling. The installer will detect an existing Cisco TMSPE SQL database `tmspe`. and you will be asked if you want to reuse this database.

Use SQL Server Management Studio to remove the `tmspe` database. SQL Server Management Studio is included with Microsoft SQL Server 2005 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	Revision	Description
January 2014	15	Added information on user access to Smart Scheduler.
December 2013	14	Updated for the release of Cisco VCS X8.1.
December 2013	13	Added Database server requirements section in Prerequisites.
October 2013	12	Updated information on editing ongoing meetings using Smart Scheduler.
September 2013	11	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	10	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	09	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 [p.10].
2013-04-24	08	Release of Cisco TMSPE 1.1.
2012-12-17	07	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	06	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	05	Clarified SQL prerequisites in requirements section. Added phone book and template upload troubleshooting scenarios.
2012-08-07	04	Added support for Cisco VCS X7.2.
2012-07-06	03	Added troubleshooting scenarios for certificate validation error and sign-in failure when no template is available.
2012-05-10	02	Added troubleshooting item for SQL Server Browser not running. Removed un-needed installation workaround for default database instances.
2012-04-27	01	Release of Cisco TMSPE 1.0.

Bibliography

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	Reference	Link
Cisco TMSPE Release Notes	D14940	http://cisco.com
Cisco TelePresence FindMe User Guide	D14958	http://cisco.com
Cisco VCS Administrator Guide	D14049	http://cisco.com
Cisco TelePresence Video Communication Server Cluster Creation and Maintenance Deployment Guide	D14367	http://cisco.com
Cisco TMS Installation and Getting Started Guide	D14389	http://cisco.com
Cisco TMS Administrator Guide	D13741	http://cisco.com
ENUM dialing on Cisco VCS Deployment Guide	D14465	http://cisco.com
How to enable Windows Installer logging	—	http://support.microsoft.com/kb/223300
Distinguished Names	—	http://msdn.microsoft.com
Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters	RFC4515	http://tools.ietf.org/html/rfc4515