Cisco TMS Provisioning Deployment Guide

D14368.05

January 2011

Cisco TMS 13 or 12.6

Cisco VCS X6 or X5.2

Table of contents

Introduction

Provisioning allows video conferencing network administrators to create and manage mass-deployable video conferencing solutions. It uses the Cisco TMS Agent to replicate and distribute the Provisioning User Directory and provisioning data from Cisco TelePresence Management Suite via a single or clustered Cisco TelePresence Video Communication Servers to endpoint devices such as the Cisco TelePresence System E20 and the Cisco TelePresence Movi software client for Windows and Mac OS X.

This guide

This deployment guide provides step-by-step instructions for installing, configuring and using provisioning to prepare and deploy Movi and E20 within an enterprise. The guide is written specifically for the software versions shown on the cover page. The table of contents indicates the sequence to take when planning and implementing a simplified provisioning deployment.

Provisioning builds upon existing capabilities in Cisco TMS and Cisco VCS, and this document assumes the reader is technically familiar with both products. It is highly recommended that only properly trained technical users upgrade, install and configure Cisco TMS or Cisco VCS for use with provisioning.

Note: Using the latest Cisco TMS and Cisco VCS software is recommended. Refer to the software release notes for each product for further detail on upgrading from prior versions to later versions of either the Cisco TMS or Cisco VCS software.

Pre-requisites

Before you begin working with Provisioning, ensure that you have:

Product	Description
Cisco TMS	Your server must be running software version 12.6 or 13.0. Servers with older major versions will require new release keys before they can be upgraded.
Cisco TelePresence Movi option keys (on Cisco TMS	One or more Movi option key(s) are needed and must be purchased separately.
Cisco VCS Control	One or more Cisco VCS Control appliances with software version X5.2 or X6 are needed. Servers with older major versions of Cisco VCS will require release keys before they can be upgraded.
Cisco VCS Device Provisioning option key	No-charge option key for your Cisco VCS Control appliance(s). Obtain this option key from your Cisco representative.

- Recommended: Microsoft Active Directory Information. If you intend to integrate the Cisco TMS User Directory with your Microsoft Active Directory so that you can automate the creation and management of users, you need knowledge of your Active Directory structure and an understanding of how AD/LDAP works. You must also define a service account in Active Directory that has read access to the Global Directory. The external AD server must support secure connections.
- Optional: SMTP Server. If you want the User Directory to email Movi users their account information including username and password, you will need to define a valid SMTP server that will accept SMTP relay from the Cisco TMS server. Some SMTP servers require authentication, so make sure you have that information before starting.
- For the proper installation of the OpenDS and Provisioning components, MS DOS or access to execute *.cmd and *.bat files (not necessarily the command prompt) must be available on the server during installation and upgrades.

Enabling Cisco TMS Agents

In Cisco TMS13.0 and 12.6 initial installs, these are disabled by default. To enable:

1. Go to **Administrative Tools > General Settings**
2. Change the **Enable TMS Agents** setting to *Yes*.

We also recommend that you proceed to confirm that the Local Cisco TMS Agent in the Cisco TMS Agent Diagnostics shows no errors and that all diagnostic tests are in the green. The Cisco TMS Agent Diagnostics can be found under **Administrator Tools > TMS Agent Diagnostics**. If any errors are found on the Local Cisco TMS Agent, these errors need to be fixed before proceeding with replication to the Cisco VCS(s). Refer to the Diagnostic section within the document for troubleshooting any errors found on the Local Cisco TMS Agent or contact your local Cisco partner or customer support for assistance.

DNS resolution for all devices

Movi and E20 are SIP-based video clients and SIP relies heavily on DNS. You will need an IP address and a DNS name for each VCS, each pool of VCSs and for the Cisco TMS server. Make sure these

DNS names resolve to the proper IP addresses before following this guide. The local hostname of the Cisco TMS server *must* match the DNS A record for the Cisco TMS Agent to operate correctly. Before starting any upgrade, ensure that the DNS servers used by Cisco TMS and Cisco VCS support both forward and reverse lookups for Cisco TMS and Cisco VCS.

Optional clustering

Each VCS can support up to 2500 video client registrations (a combination of Movi clients and any other compatible H.323/SIP endpoints or infrastructure). Up to six VCS peers can be combined in a single cluster, supporting a maximum of 10,000 video client registrations (the 5th and 6th peers in the cluster provide resiliency rather than increased capacity).

If you are intending to provision from a cluster of Cisco VCSs, configuration of the cluster is a separate process. You can either create the cluster after enabling provisioning or configure provisioning after creating the cluster. Details on how to create a cluster can be found in the *Cisco VCS deployment guide—Cluster creation and maintenance*. Make sure you choose the document version corresponding to your Cisco VCS version.

Ports used by the Cisco TMS Agent

The Cisco TMS Agent uses the following ports:

Port	Description
389	Locally on both the Cisco TMS and all Cisco VCSs.
8787	Locally on both the Cisco TMS and all Cisco VCSs.
4444	The administrative port for the Cisco TMS Agent used between all replicating partners to accomplish for example a change of password, initial replication to VCS (for example, authentication). The traffic exchanged on this port is encrypted.
8989	The replicating port used between all replicating partners. The traffic exchanged on this port is encrypted.
4444 and 8989	Both port 4444 and 8989 are used during initial replication setup; port 4444 for the administrative functions, and port 8989 for the data.

Software dependencies and upgrades

There is a software dependency between Cisco TMS 12.6 and VCS X5. If your installation already uses the Cisco TMS Provisioning Directory functionality for Cisco Movi or E20 deployments and you are upgrading Cisco TMS from versions earlier than 12.6, you must follow the upgrade procedures in the document *Cisco VCS Cluster Creation and Maintenance Deployment Guide*.

WARNING: Upgrades will be blocked if the procedures in these documents are not followed. The error messages state that Provisioning on all clusters must be disabled before upgrading to Cisco TMS software version 12.6 or from versions pre-12.6 to 13.0.

Configure Cisco VCS for provisioning

There are two types of Cisco VCSs:

1. Cisco VCS Control is designed to be installed behind the organization's firewall to provide registration and routing capabilities to Movi and H.323 and SIP based endpoints used within the business or connected over a VPN into the business.
2. Cisco VCS Expressway is designed to be installed on the outside (public side) of an organization's firewall to provide registration and routing capabilities for public and home based Movi and H.323 and SIP based endpoints. The Cisco VCS Expressway also provides firewall traversal capabilities to allow communication with the internal Cisco VCS Control and endpoints that are registered to it.

Provisioning should only be enabled on Cisco VCS Control units. If Movi is registered to a VCS Expressway, provisioning requests will be automatically forwarded to the Cisco VCS Control associated with the Expressway via the appropriate traversal zone.

Note: If provisioning is enabled on a VCS Expressway or any other VCS that does not need to have provisioning enabled, be sure to disable it by using the process specified in Removing provisioning from a VCS.

Synchronize time in Cisco VCS and Cisco TMS

Time needs to be synchronized in Cisco VCS and Cisco TMS. Cisco recommends keeping time synchronized using an NTP (Network Time Protocol) server. If possible, both Cisco TMS and Cisco VCS should use the same NTP server.

- Cisco TMS uses the NTP settings for the host Windows Server Operating System. To configure the Windows NTP setting, see this Microsoft help article (http:/support.microsoft.com/kb/816042).
- To configure the NTP server on the Cisco VCS, go to **System Configuration > Time**.

More information about NTP servers can be found at http://www.pool.ntp.org.

Setting up DNS for the Cisco VCS

The 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 Configuration > DNS**.
2. Set 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 VCS (typically the same as the **System name** in **System configuration > System**, but excluding spaces).
4. Set **Domain name** so that <Local host name>.<DNS domain name> is the unique FQDN for this VCS.
5. Click **Save**

Enable Device Provisioning on Cisco VCS Control

Provisioning is activated by installing the Device Provisioning option key on the Cisco VCS Control (not on Cisco VCS Expressway). Contact your Cisco representative for more information on how to obtain the Device Provisioning option key.

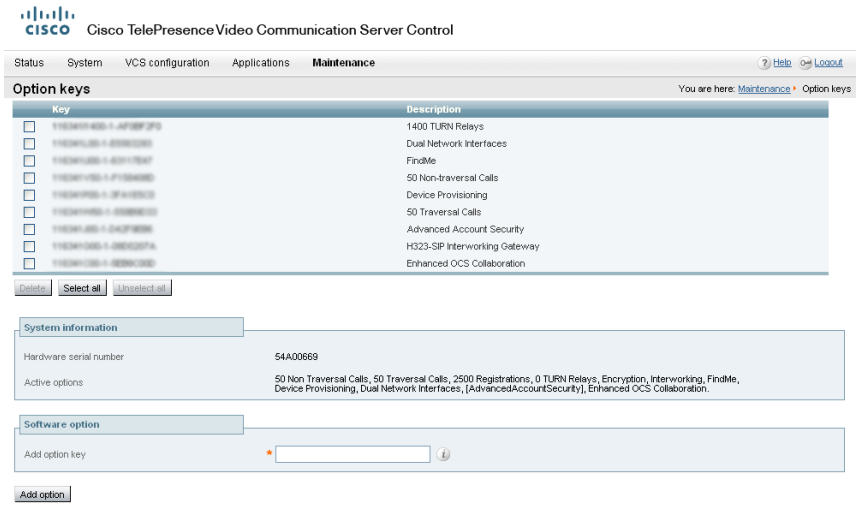
Installing the Device Provisioning option key

Option keys can be installed in three ways, described below.

Note: 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.

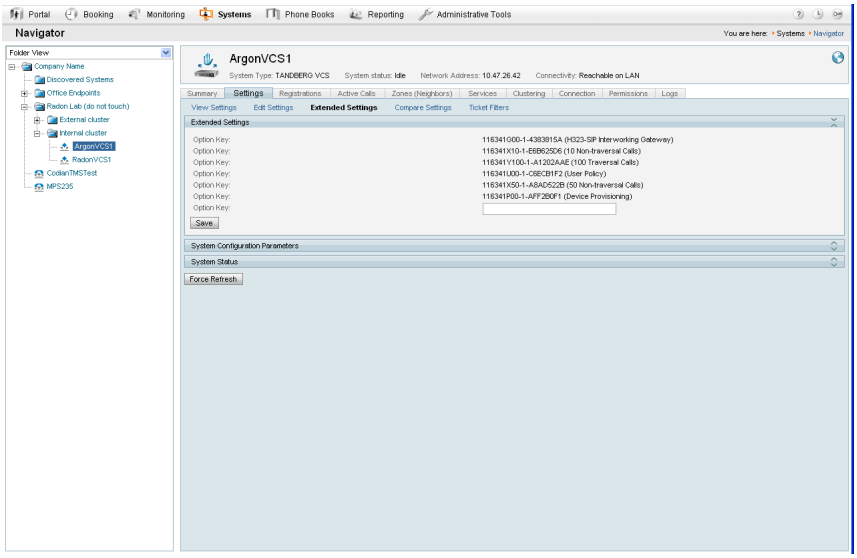
A. Adding option key via the VCS web interface

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 wish to add.
4. Click **Add option**.



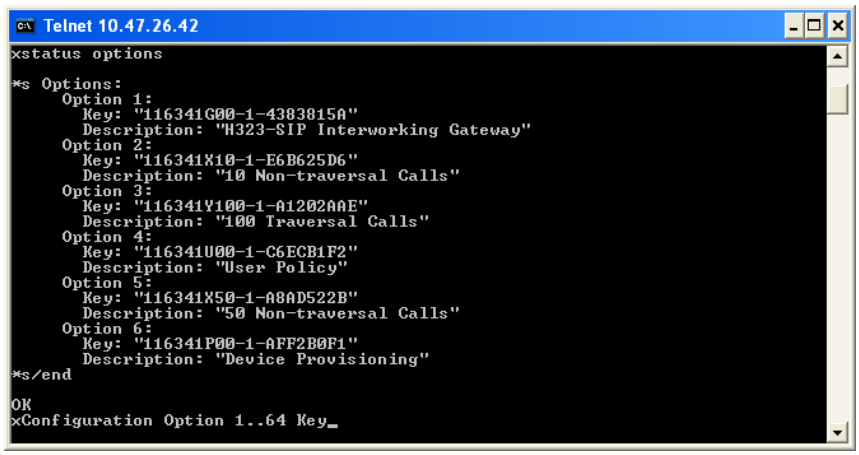
B. Adding option key via Cisco TMS

1. In Cisco TMS, go to **Systems > Navigator > Folder View**.
2. Select a VCS.
3. Select the **Settings** tab.
4. Click **Extended Settings**.
5. Enter the option key.
6. Click **Save**.



C. Adding option key via the Cisco VCS command-line interface

1. To return the indexes of all the option keys that are already installed on your system, type: **`xStatus Options`**
2. To add a new option key to your system, type: **`xConfiguration Option [1..64] Key`**



Warning: When using the CLI to add an extra option key, you can use any unused option index. If you choose an existing option index, that option will be overwritten and the extra functionality provided by that option key will no longer exist. To see which indexes are currently in use, type **`xConfiguration option`**.

After installation

After the Device Provisioning option key has been installed, wait 10 minutes to make sure that the installation process has completed. In the VCS event log, immediately after enabling device provisioning, you will see

Event="Directory Service Starting" Detail="The directory service is starting"

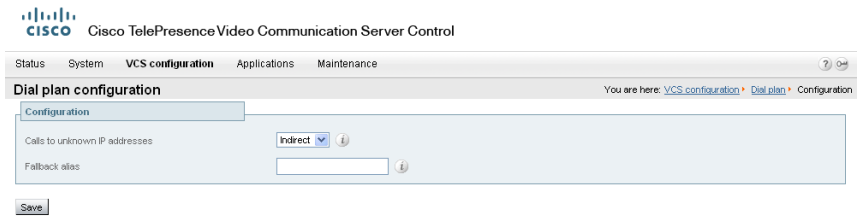
Enable SIP on Cisco VCS Control and Expressway

In each VCS:

1. Ensure SIP mode is turned on (**VCS Configuration > Protocols > SIP > Configuration**). By default this is turned on. See the *Cisco VCS Administrator Guide*.
2. Ensure the SIP domain is specified (**VCS Configuration > Protocols > SIP > Domains**).

Set up Cisco VCS calls to unknown IP addresses

Cisco VCS Control should use the *Indirect* mode for **Calls to unknown IP addresses**. This is configured in **Configuration > Search rules > Configuration.**



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

Adding the Cisco VCS to Cisco TMS

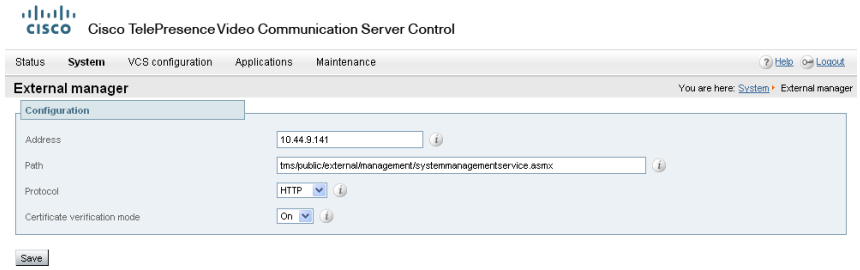
This procedure is compulsory for the Cisco VCS Control, and optional for the Cisco VCS Expressway.

In each Cisco VCS:

- Optionally, ensure that SNMP is enabled (Enabled = On) and an SNMP community name is set on the Cisco VCS (**System Configuration > SNMP**). This is the best way for Cisco TMS to be able to detect and add the Cisco VCS.

  Note: 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.

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

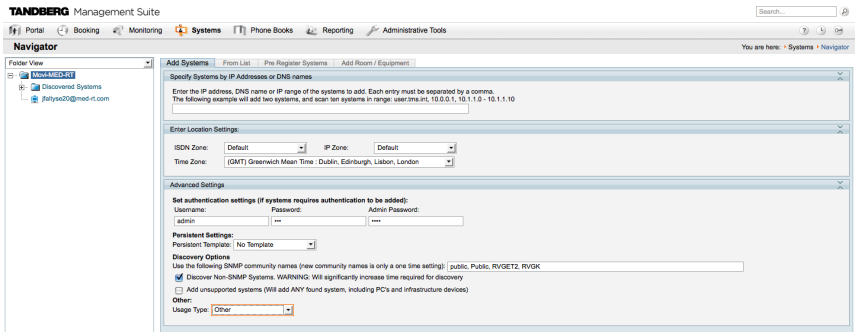


In Cisco TMS, add the Cisco VCS:

1. Cisco TMS **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, simply input the Cisco VCS IP Address and click **Next**. Cisco TMS will collect information from the Cisco VCS about how best to communicate with it.

   Note: If you do not support SNMP on your network, the Cisco VCS can be discovered using alternative means in Cisco TMS. See the section on discovering non-SNMP devices in the Cisco TMS Administrator Guide.

4. Click the button **Add Systems** in the right pane. Follow the instructions in Cisco TMS to add the Cisco VCS.



5. Ensure that the Host Name of the VCS is set up in Cisco TMS:
   a. Go to **Systems > Navigator**.
   b. Select the Cisco 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**. You may get an error message saying "DNS config failure resolving <DNS name>: Did not find system IP address () in DNS: <Server IP>". This message can safely be ignored.
8. Ensure that Cisco TMS updates its DNS:
   a. Select the **Settings** tab.
   b. Click **Force Refresh**.

Enable provisioning on the Cisco VCS Control

Only Cisco VCS Control requires this configuration. Cisco VCS Expressway must not have provisioning enabled.

WARNING: 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 cluster and your Cisco VCS Control is not currently part of one, complete the configurations described below, and afterwards set up the cluster as described in *Cisco VCS Deployment Guide—Cluster creation and maintenance*.

Setting up a cluster name

If FindMe™ is to be used, the Cisco VCS must be set up 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 pool of Cisco VCSs managed by this Cisco TMS.
- identical to the SIP server address configured in Cisco TMS (**Systems > Provisioning > Directory > Configurations** pane, the **SIP Server Address** field).

If a cluster name exists, but is different from the SIP server address, it must be changed so that they are identical. To set up or change the cluster name:

1. Go to **VCS Configuration > Clustering**
2. Add a **Cluster name**:
   a. 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".
   b. 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**.

Moving FindMe™ data

Once the cluster name has been set up/edited, use the movefindmedata script to move the FindMe™ data to use this new name, using the process defined in *Cisco VCS Cluster Creation and Maintenance Deployment Guide*.

Note: Failure to follow the instructions in *Cisco VCS Cluster Creation and Maintenance Deployment Guide* will cause FindMe™ users to be lost.

Cisco VCS is not part of a cluster

To enable provisioning on a VCS Control that is not part of a cluster:

1. In Cisco TMS, go to **Systems > Navigator > Folder View**
2. Select the VCS Control (not Expressway). This displays the device page.
3. Select the Cisco TMS Agent tab.
4. Click Enable Cisco TMS Agent Data Replication. This may take a while to complete (approximately 5 minutes, see note on **Activity Status** below).
5. Click **Save**.

Note: In Cisco TMS, go to **Administrative Tools > Activity Status** to see activities that are active, scheduled or in progress. Selecting the activity **Enable TMS agent data replication for system(s) <name of system>** will display an activity log for this event. When finished, the activity will say ‘Event completed successfully'. You may need to click **Refresh** to get a real time update.

Cisco VCS is part of a cluster

To turn on provisioning for the cluster:

1. In Cisco TMS, go to **Systems > Navigator > Folder View**
2. Select the Master VCS Control (not Expressway). This displays the device page.
3. Select the **Clustering** tab.
4. Ensure that **Enable TMS Agent Data Replication on all cluster members** is selected. This may take a while to complete (see note on **Activity Status** above).
5. Click **Save Cluster Settings**.

Enable replication (recommended)

By enabling replication, Cisco TMS makes sure that the connected VCSs get configured with the relevant details. On the same screen, you also make sure your endpoints gets to be authenticated at log on.

In Cisco TMS, for each VCS (one if the VCS is not in a cluster, up to 6 if a cluster of VCSs is being configured):

1. Go to **Systems > Navigator > Folder View**.
2. Select the VCS.
3. Select the **Cisco TMS Agent** tab.
4. For **Authentication Scheme**, select *Digest* for authentication of endpoint.
5. Ensure that **Enable Cisco TMS Agent Data Replication** is selected.
6. Click **Save Settings**.

Change LDAP Configuration and Replication passwords (recommended)

It is recommended that the LDAP Configuration Password and the LDAP Replication Password are changed from the default setting of Cisco. Changing the values on Cisco TMS will propagate the changes to all Cisco TMS Agents both on the Cisco TMS(s) and VCS(s).

In Cisco TMS:

1. Select **Administrative Tools > Configuration > Cisco TMS Agent Settings.**
2. In the **Global** (applied to all agents) pane:
3. Enter the new password in the **LDAP Configuration Password** field.
4. Enter the new password in the **LDAP Replication Password** field.
5. Click **Save**

Note: Cisco recommends that the **LDAP Configuration Password** and **LDAP Replication Password** be different. Ensure that these passwords are noted and secured appropriately.

Provisioning status

After provisioning on the cluster is complete. In Cisco TMS:

- You can view the replication status of the cluster from the **Administrative Tools > Cisco TMS Agent Diagnostics > Cisco TMS Agent** tab.
- From the same location you can click the **TMS Agent Diagnostics** link located next to the **TMS Agent Configuration** link at the top of the tab.

On Cisco VCS:

- You can click the link **View TMS Agent replication status** on the **VCS configuration > Clustering** page.

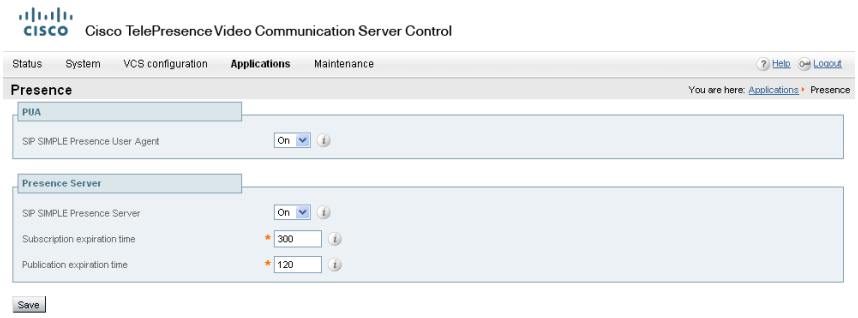
See Diagnostics for more information concerning Cisco TMS Agent Diagnostics.

Enable Presence on the Cisco VCS (optional)

Movi can use the Cisco VCS as a presence server to share presence information (for example Offline, Online, Away or Busy) with other users.

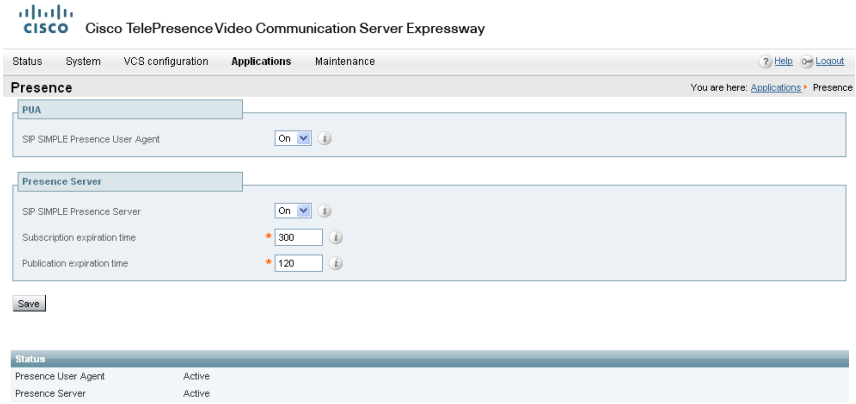
Presence on Cisco VCS Control

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



Presence on Cisco VCS Expressway

If Cisco VCS Expressway is to publish presence (Offline, Online and Busy) on behalf of endpoints registered to it that do not publish their own presence, you must also set **SIP SIMPLE Presence User Agent** to *On*.



Note: The SIP SIMPLE presence server must not be enabled on Cisco VCS Expressway; the Cisco VCS Expressway must pass presence information to the Presence Server on Cisco VCS Control rather than keep the presence information locally.

Create and manage user accounts

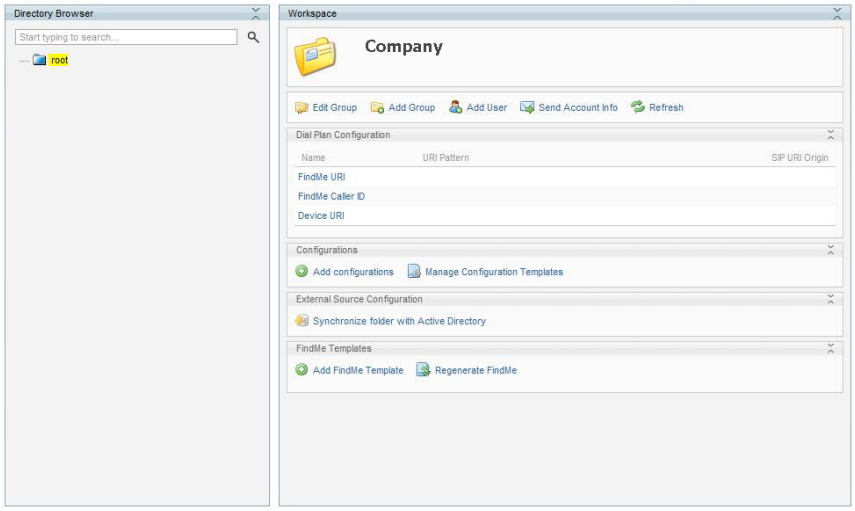
Overview of the Provisioning Directory

Location in Cisco TMS: **Systems > Provisioning > Directory**.

- The **Directory Browser** pane on the left side of the screen initially displays a group (folder) called root. This represents the main organization name; for example in the picture below we've clicked on the folder name root and changed it to *Company*. The root folder cannot be deleted.
- The **Workspace** pane on the right side of the screen has five subsection panes (at root) where you will perform the major part of your tasks. The subsection panes and the tasks you can complete in each of these subsections are explained in more detail below.

Note: You will only see the **FindMe Templates** pane when the root folder is selected. You will only see the **External Source Configuration** pane when a folder is selected. When you select a user in the **Directory Browser**, you will not see **External Source Configuration** or the **FindMe Templates** panes. However, the **Devices** subsection pane is seen showing the user's provisioned devices. FindMe will not be seen if **FindMe Enabled** is *No* (default is *Yes*) under **Administrative Tools > Configuration > TMS Agents Settings.**

Information pane for a group or user



When a group is selected in the Directory Browser, the following options are available in the information pane:

- **Edit Group**: changes the group name.
- **Add Group**: adds a group under the currently selected group in the Directory Browser
- Edit the group name by selecting **Edit Group**.
- Add a group by clicking **Add Group**. The group will be added under the group you have selected in the Directory Browser.
- Add a user manually by clicking **Add User**. The manually created user will be added in the group you have selected in the **Directory Browser**. Creating manual users is discussed later in the chapter.
- Configure email settings and send account information to users by selecting **Send Account Info**. Configuring email settings is discussed later in this chapter.
- Refresh the pane by clicking **Refresh**.

When you select a user in the **Directory Browser** of the Information pane, you can:

- Show and hide user details by selecting **Show Details**.
- Edit the user by selecting **Edit User**. If the user is being imported from Active Directory, only **Password**, **User ID** and **Image URL** are editable.
- Delete a user by clicking **Delete**.
- Send the user's account information to the selected user by clicking **Send Account Info**. Note that email settings must be configured for this to work.
- Refresh the pane by clicking **Refresh**.

Dial Plan Configuration Pane

The **Dial Plan Configuration** pane is where you configure your FindMe URI, FindMe Caller ID and Device URI.

- FindMe URI is the template for creating the FindMe™ ID names.
- FindMe Caller ID is the number the Cisco VCS will report as the callback number when calling out of gateways.
- Device URI is the template for creating the name of provisioned devices.

You can use the following user information fields to generate the URI pattern for **FindMe URI** and **FindMe Caller ID**:

- emailAddress (default)
- username
- lastName
- firstName
- officePhone
- mobilePhone

To create the URI pattern for **Device URI** you can, in addition to the above, use the following device information:

- model (device.model)
- connectivity (device.connectivity)

For example:

1. Mouse over and select **Edit**

2. Edit the **FindMe URI Pattern** appropriately.

Recommended: {emailAddress}

The email address domain should be the same as the SIP Domain.

Alternative: {username}@<domain>

<domain> is the SIP domain configured on your Cisco VCS (in Cisco VCS go to **VCS configuration > protocols > SIP > Domains)**.

WARNING: If {username} is utilized for the FindMe URI Pattern, we recommend that the @ symbol not be included in the {username}.

Cisco recommends that you use the default Device URI Pattern ({username}.{device.model}@company.com) to easily identify the type of device the user provisions to (that is, 'movi' or 'e20') and to maintain unique Device URI Patterns.

WARNING: If one or more users have the same Device URI, this will create problems with user reporting in Cisco TMS, as the lookup from URI to username can only return one of the users with this URI.

The default action when clicking on links in the **Dial Plan Configuration** pane is to edit the particular pattern.

If you want to clear a pattern for a certain group or user, you can leave it empty and save it. This will override any value from a parent group.

If you want to delete a pattern on a certain group or user, mouse over the link, click the drop-down icon and select **Delete**.

Note: If the pattern is not set on the given level, the delete action will not be available. For the root group, trying to save a blank pattern or removing it will result in the same behavior.

Regex

Regex is supported for the URI value mappings both in the **Dial Plan Configuration** pane and the FindMe Templates is supported.

Examples

To remove spaces:

```
{mobilePhone[' '='']}@company.com
```

To remove spaces and +47:

```
{mobilePhone[' '='','\+47'='']}@company.com
```

To extract the domain part of the email address:

```
{username}.office@{User.emailAddress['^.+?@'='']}
```

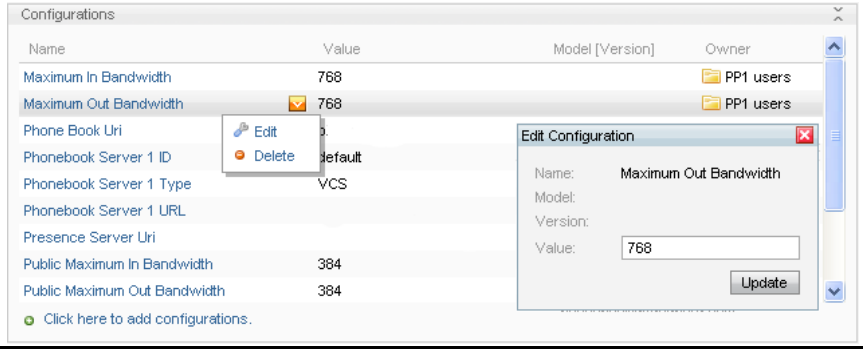
To replace ø with o:

```
{username['ø'='o']}@company.com
```

Configurations Pane

Edit Configurations

To edit the current configuration, mouse over the configuration's name and click the arrow that appears to the right and click **Edit**. Edit as required and click **Update**.



Note: We strongly recommend that configurations be modified independently of endpoint and software version. Add the configuration on the highest level possible to simplify management and upgrades to new versions that add new configuration templates.

Delete Configurations

When deleting a configuration, it's important to understand at what level you're deleting it and where the configuration was set, that is, at the root level, the folder level or the user level.

For example, if you have set configurations at the root level and they are propagating down to folders or users directly under it, you will get this warning if you select a lower level and attempt to delete the configuration from there:

However, if you delete that Configuration at root level, you will not receive this warning, and the changes will propagate downwards to any folders or users under the root level folder appropriately.

Upload new configuration template

1. Go to ftp://ftp.tandberg.com/pub/software/tms.
2. Locate and download the configuration templates to your local server.
3. Click **Manage Configuration Templates**.
4. Click **Upload New**.
5. Locate and select the configuration template.
6. Click **Open**.

The new configuration template is now in your list of templates.

Best practice for configuration template management

While each version of an endpoint's software will usually have its own configuration template, we recommend that "old" templates are cleaned out regularly as the corresponding versions are phased out in your organization.

External Source Configuration pane

The **External Source Configuration** pane is where you will configure the Active Directory information to import user information from AD to the Provisioning Directory. Cisco highly recommends utilizing AD to import users. See the section below called Recommended: Automated user creation and management with Microsoft Active Directory for further detail.

FindMe Templates pane

In the **FindMe Templates** pane, the administrator can now specify zero or more FindMe templates. All new users within your folder structure (from root down) will get a FindMe profile created from the FindMe profile template upon creation. For example, on each template you can set up zero or more FindMe device templates. These will let you define a sensible default configuration based on the company's existing dial plan.

Automated user creation and management with Microsoft Active Directory (recommended)

The User Directory in Cisco TMS used for provisioning supports integration with Microsoft Active Directory for the creation and management of users, making provisioning large numbers of users easy and scalable. Cisco highly recommends this for the power and flexibility of AD in the solution.

Users imported to the User Directory in Cisco TMS will show up with gray shirts, while manually created users show up with blue shirts. For information concerning the manual creation of users, see the section called Manual user creation and management (optional).

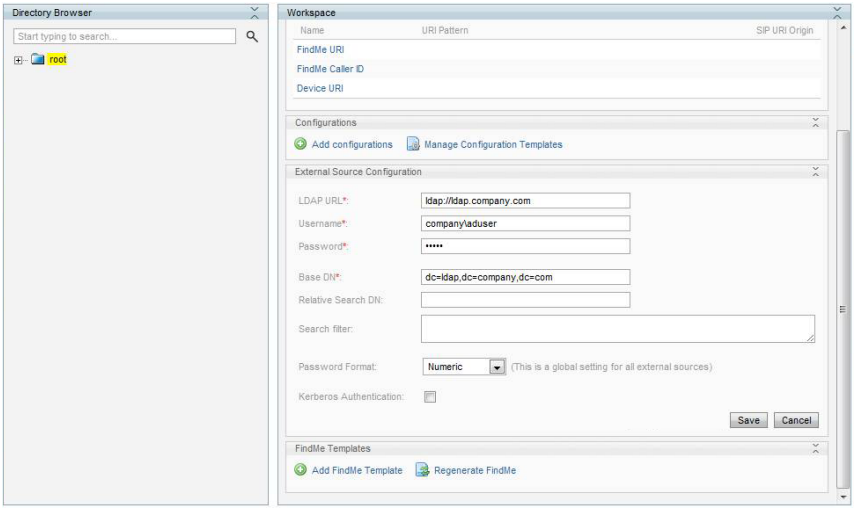
Once configured, the User Directory will automatically synchronize with Active Directory once a day. The time of the update is displayed on screen. Currently, this automatic synchronization cannot be changed, but you can run the AD synchronization manually at any time. Cisco recommends running manual synchronizations at the highest group folder level possible according to your External Source Configuration plan.

For example, if your External Source Configuration begins importing users at root and you have created search filters that place users in sub group folders under root, then you should run the manual synchronization from root. You can also run a manual synchronization at the sub group folder level, but ensure that your AD search filter is correct for that level before proceeding.

Note: Only user names and those fields shown in Mapping of user fields are synchronized—the user's AD password is NOT imported into the User Directory. Provisioning will automatically assign a user's Movi password. For more details on mapping of user fields between Active Directory and the Provisioning Directory database, see Mapping of user fields.

Familiarity with Microsoft AD and LDAP is required to synchronize users.

1. Select the root folder.
2. Click on the **Click to synchronize this folder with Active Directory** link to go to the **Edit** screen.
3. Enter the LDAP URL to an Active Directory Global Catalog Server and provide the Global Catalog Port Number (default 3268), for example LDAP URL: ldap://globalcatalog.company.int:3268
4. Enter the **Username** to use when logging on and importing from Active Directory. Cisco recommends that this user be the Service Account and that password retention policies are not applied to it.
5. Enter the **Password**.
6. Enter the selected **Base DN**, for example dc=ldap,dc=company,dc=com.
7. If necessary, enter the selected **Relative Search DN**, for example OU=users.
8. Click **Save**.

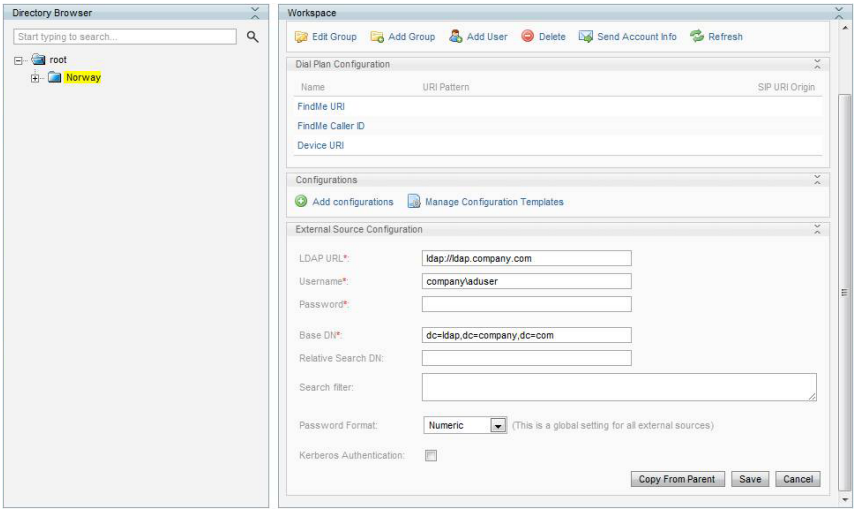


To import users immediately:

1. Click the link **Click here to import all users from this source**.
2. Wait for the import to complete. This could take some time depending on the number of users you are importing.
3. Click **OK**.
4. Refresh the browser. You should now see users imported to the root folder in the Directory Browser pane. AD users imported to the Provisioning Directory Browser show up with gray shirts.

To manage AD Sync at a sub-group level:

1. Create a sub-group under the root group folder, for example Norway.
2. Select the group folder you created to edit that group's AD sync.
3. **Click to synchronize this folder with Active Directory**.
4. Click **Copy From Parent** (this information is filled in automatically from the parent folder, if applicable)



5. Enter a Search Filter according to the group's LDAP definition in AD. For example, you might have a location set to cn=no to import all users in Norway to this sub-group.
6. Click **Save**.

Note: When synchronizing folders in the sub-group levels, and after the synchronization is complete on a sub-group level, a force refresh of the GUI is required. Force refresh must be done to correctly view any actions (for example moving users between folders) that may have occurred during the operation. Doing a force refresh of the GUI will return the highlighted cursor to the Root level.

To import users immediately to this group, return to the root level, then

1. Click the link **Click here to import all users from this source**.
2. Wait for import to complete.
3. Click **OK**.
4. Refresh the browser.

Note: If the user was initially imported by the first synchronization to the root group folder, but the user also belonged to the AD CN search filter for the Norway group folder, the user will automatically be moved from the root group folder to the Norway group folder at the next synchronization.

If AD Security Groups or AD Distribution Lists are used to import users to the Cisco TMS Provisioning Directory, it is recommended not to use the **Relative Search DN** field, but instead create a filter in the **Search filter** field. For example, and let's assume you require to search on a security group in AD, then you would enter the **Base DN** (for example dc=eu, dc=company, dc=com), leave the **Relative Search DN** blank and in the **Search filter**, enter your search, for example memberOf= cn=videoconfusers, ou=security groups, dc=subdomain, dc=domain.

Kerberos authentication

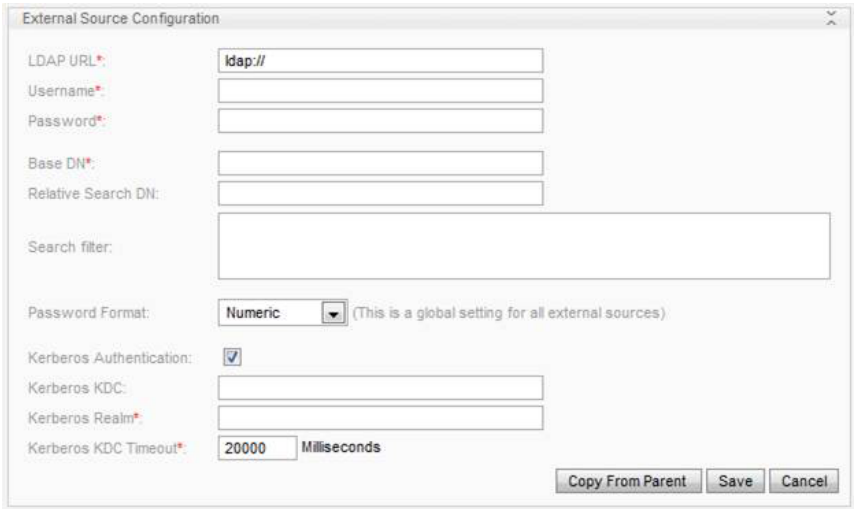
To import users using a secure connection, Cisco TMS supports Kerberos authentication towards AD.

To enable and configure, use the **External Source Configuration** pane.

1. Click the **Edit** button.
2. Check the **Kerberos Authentication** check box and enter the required settings.

The required settings are:

- **Kerberos KDC**: (Key Distribution Center): The address of the Kerberos KDC server, which is the address of your Active Directory (AD). The value can either be a fully qualified domain name (FQDN) or the domain your AD server resides, in which case a DNS SRV lookup is performed to determine the FQDN.
- **Kerberos realm**: The realm configured in AD for Kerberos Authentication.
- **Kerberos KDC timeout**: The maximum number of milliseconds to wait for a reply from the KDC.



Mapping of user fields

The table below shows the mapping of fields between Active Directory and the database in the Cisco TMS Provisioning Directory.

Provisioning Directory LDAP field	Workspace attribute	Active Directory attribute	Comment
username	Username	sAMAccountName	
emailAddress	Email address	mail	
externalId		objectGUID	The objectGUID is prefixed with the LDAP URL the user was imported from.
firstName	First Name	givenName	
name	Displayname	displayName	If displayname is null or empty, user.username is used.
lastName	Last Name	sn	If sn is null or empty, username is used.
title	Title	title	
company	Company	company	
department	Department	department	
officePhone	Office Phone	telephoneNumber	
mobilePhone	Mobile Phone	mobile	

Note: As a minimum, the sAMAccountName and mail attributes are required to import to the Cisco TMS Provisioning Directory appropriately. Cisco TMS also filters out anything that is disabled in AD, meaning that if the account is disabled, Cisco TMS does not import it. In addition, if the account was active and imported to the Provisioning Directory and then disabled, Cisco TMS will remove it from the Provisioning Directory at the next synchronization.

Manual user creation and management (optional)

While we strongly recommend using Microsoft Active Directory to import your users to the User Directory, the manual creation of users in the Provisioning Directory is supported.

Manual creation of users can replace or be combined with AD import. This requires more effort on the part of the administrator, who will need to manually create these users in the User Directory as well as create FindMe accounts for the users on the Cisco VCS Control, if necessary. In addition, manually created users cannot be moved between group folders. When importing from AD, this can be done based on search filters used in your **External Source Configurations**, as explained earlier in this chapter.

To create a user, select the group folder you want the user in, then do the following:

1. Click **Add User**.

2. When the **Workspace** pane appears, enter a name for user and then the user's details appropriately. **Email Address**, **Username** and **Password** are all required fields.
3. Click **Save**.

Note: The User ID field defaults to zero (0) when manually creating a user, and if left at 0, a user ID will be automatically generated by Cisco TMS when the user is saved. Cisco recommends allowing Cisco TMS to generate these IDs, as they should be unique to each user.

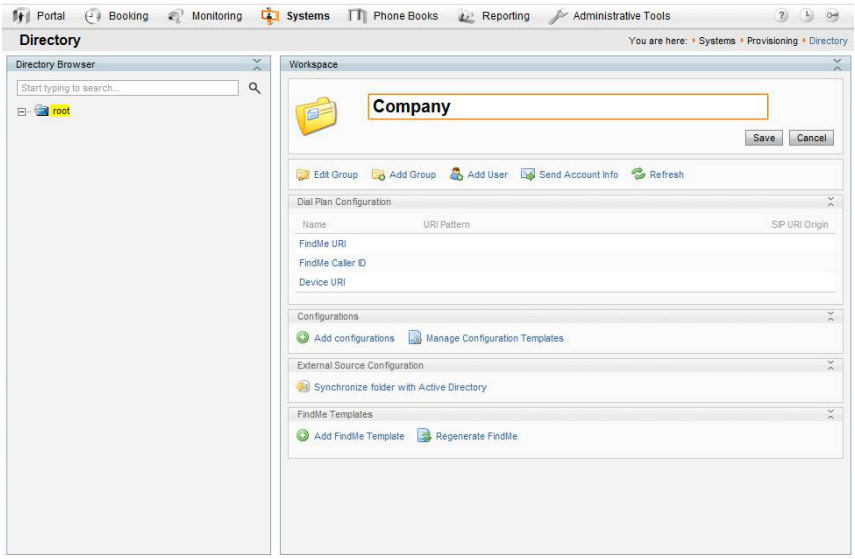
This finalizes the provisioning setup in Cisco TMS. The settings that were configured during this process will now be replicated to the Cisco VCS or cluster of Cisco VCSs by the Cisco TMS Agent. Any future configuration changes made in the Provisioning Directory UI in Cisco TMS will be replicated to the Cisco VCS or cluster of Cisco VCSs again by the Cisco TMS Agent.

The Cisco TMS Agent replicates through a multi-master replication process, meaning that no one database is the master of all. The Cisco TMS Agents on the Cisco TMSs (if in a Cisco TMS redundant setup) and Cisco VCSs (if in a cluster) continually check with one another for changes and differences between them. All provisioning configuration changes must be made via the Cisco TMS Provisioning Directory UI.

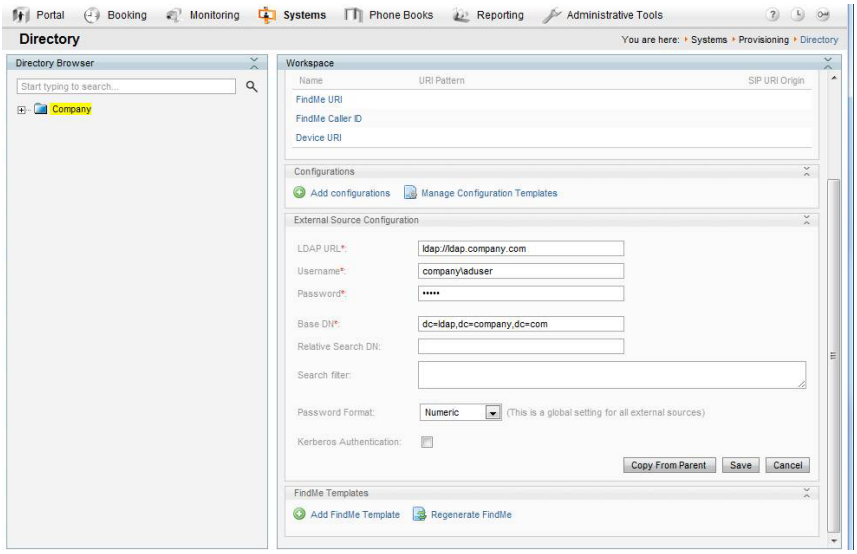
User Directory configuration—an example

The following is an example of a possible Movi/E20 deployment.

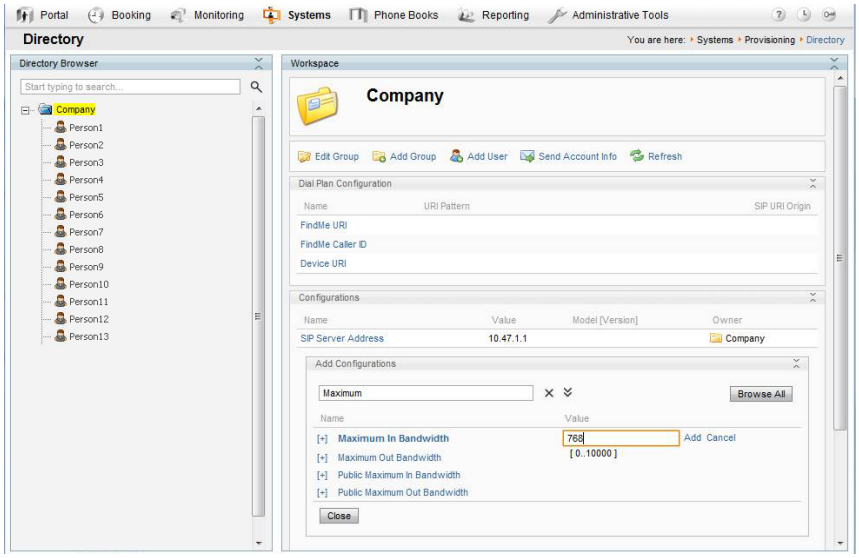
Tore is the administrator and responsible for setting up provisioning in our example. His company has about 20 users located in Norway and India. The first thing he wants to do is set up basic provisioning for all his users. He starts by giving the root folder a name by choosing **Edit Group** in the **Workspace** pane:



As recommended, he then configures the external source connection on the root folder to import his users from Active Directory:



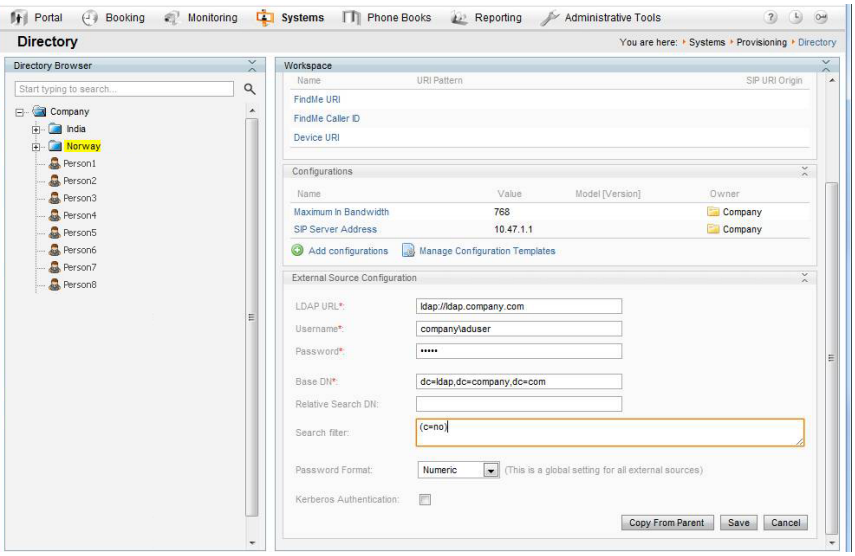
Once the users are imported from AD, he starts configuring the settings he wants to provision the Movi clients with, for example **Maximum In Bandwidth:**



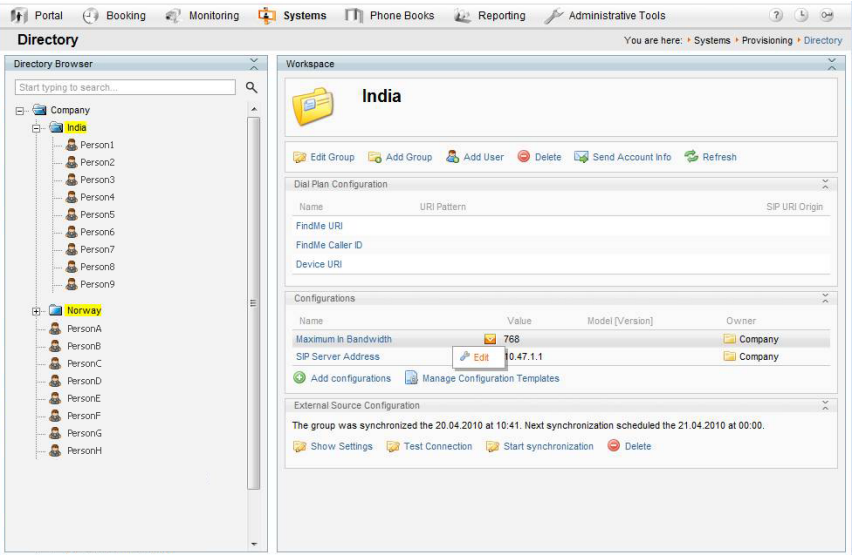
He then realizes that the users in India have a limited connection compared to their Norwegian counterparts. To configure the Indian users differently from the Norwegian ones, he creates two new groups under the root group called "Norway" and "India".

He chooses the Norway group and selects **Click to synchronize this folder with Active Directory**. The settings he used to synchronize the root group are exactly the same as for the Norway group, so he clicks **Copy From Parent**. All he needs to do now is edit the password and the Search Filter.

Tore is familiar with his AD and knows that to import the users from Norway, he needs to set the search filter to cn=no, and to import the Indian users he needs the search filter cn=in.



Once he has configured both new groups, he clicks **Start Synchronization** at the root level (Company) to ensure that all groups are synchronized correctly. He should now see that all users are moved to their correct group.



He can then override the bandwidth setting he set on the root group with a lower bandwidth setting on the India group. The Norway group will still use the setting from the root group.

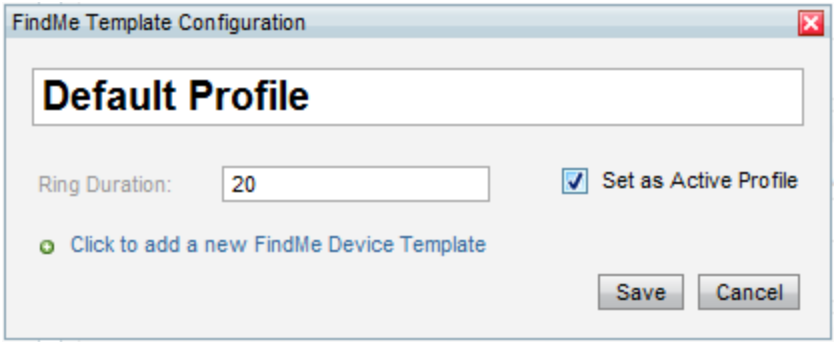
In the future, if he ever needs to configure some users differently in the same country, he would simply have to create a group for them, and configure the Search Filter so that it imports just the users he wants to treat differently. For example:

- Import only the users in the Indian R&D department: (&(c=in)(department=R&D))
- Import only the Indian users whose names begin with A: (&(c=in)(name=a*))

FindMe configuration—an example

Next, Tore wants to set up FindMe to automatically include all the endpoints they have in his company. For example, some of his users have endpoints form the MXP Series and these devices have URIs on the form: **<username>.office@company.com**

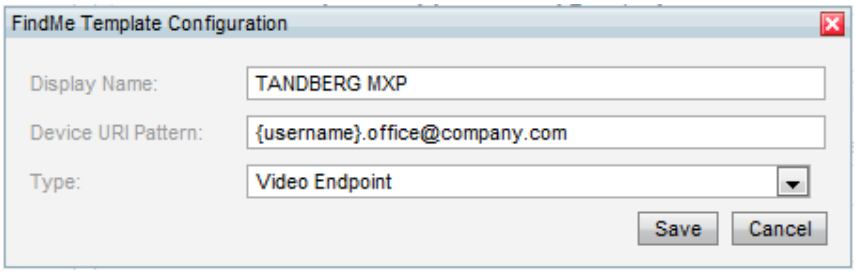
Tore goes to the root group and clicks **Add FindMe Template**which displays the popup below:



He then gives the FindMe Template a name, and chooses to use it as the active profile. He then clicks **Save**.

He will have to add a FindMe Device Template to his FindMe Template for the Cisco TelePresence System MXP Series endpoint. He clicks **Edit**, and then **Click to add a new FindMe Device Template**.

He gives the device a name, the Device URI pattern {username}.office@company.com and the correct type:



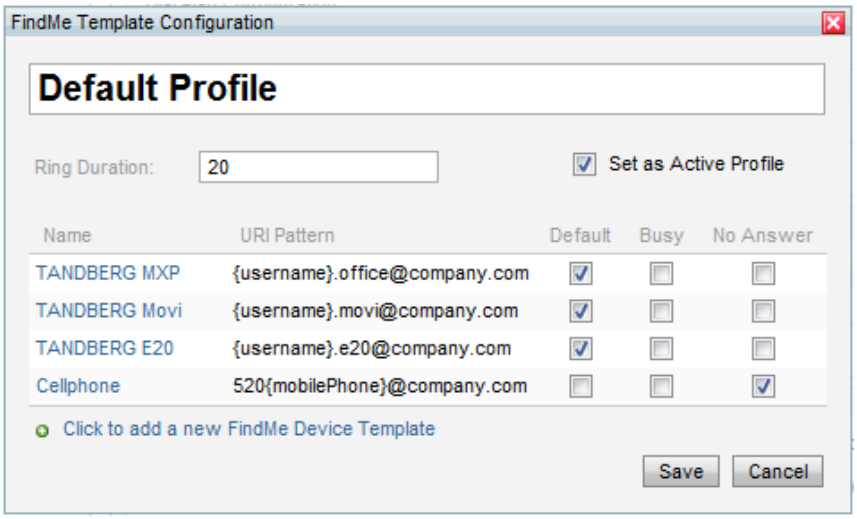
As Tore has both Movi and E20s in his deployment, Tore also needs to set them up to be provisioned. In the **Dial Plan Configuration** pane, he has set the Device URI Pattern to be provisioned with:

{username}.{device.model}@company.com
{device.model} will be replaced with "movi" or "e20". To add support for these, he must create two more FindMe Device Templates with the following URIs:

{username}.movi@company.com{username}.e20@company.com
In addition, he has an ISDN gateway installed, and wants all calls to be redirected to the users' phone if they don't answer within the current limit of 20 seconds. He therefore configures another device with the following URI:

520{mobilePhone}@company.com
This pattern will get the user's mobile number as configured in AD, and add 520, which is the prefix for Tore's ISDN gateway, in front of it.

Finally, he sets the devices to dial by default when someone calls a user's FindMe address, and he specifies that the mobile phone be called if the call isn't answered by any of the other devices:



When he is finished, he saves the settings and closes the dialog window.

To create the actual FindMe Profiles and FindMe Devices from the templates he configured, he must click **Regenerate FindMe**. All users will be created with each device address contained in the template even if they don't physically have all the devices.

Note: We recommend that whenever changes are made and saved in the FindMe Template Configuration, the Administrator selects **Regenerate FindMe** to ensure all changes are updated appropriately. Selecting **Regenerate FindMe** will replace existing FindMe users' configurations as well as apply configurations to any new users.

Tore has now imported users from AD, created a dial plan, system configurations and FindMe templates. Now he needs to send the users their account information details.

Sending account information

Before account information can be sent to the users, email settings must be configured in the Provisioning Directory:

1. In Cisco TMS, go to **Systems > Provisioning > Directory**.
2. Select the root folder.
3. Click **Send Account Info**.
4. Click **Configure Email Settings**.
5. Enter the appropriate information (see below).
6. Click **Save**.

Message template

The message template must at least include the parameters for username: {username} and password: {password}.

If you have configured FindMe for your users, then we also recommend that you include a link to the user FindMe configuration on the Cisco VCS in the email message.

Test and send

To test that email settings are working correctly, select yourself (or a suitable user) from the Directory Browser, then click **Send Account Info**. The **Send Account Information** window will open, where you may click **Send Email**. Once you have confirmed that this email message was received correctly by you or your test user, you are ready to send all users their account information.

To do this, simply select the root folder and repeat the above tasks to send account information to all users.

Note: When a new user is included in the Provisioning Directory, either manually or imported from AD, the administrator must manually send the account information to the new user.

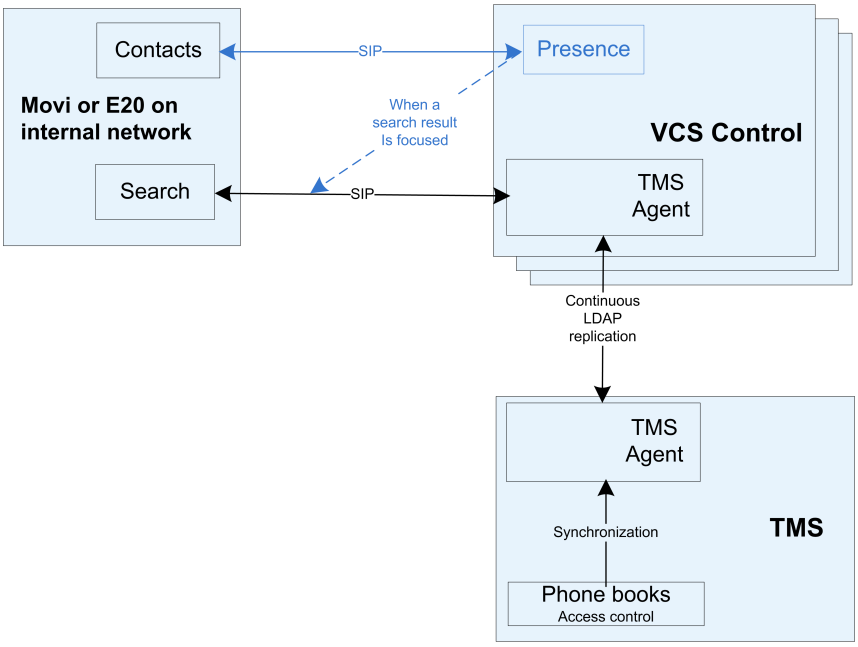
Phone Books for Movi and E20

Unlike for other systems in Cisco TMS, you don't "set" phone books to Movi or E20. The Phone Book Uri you add in the Configurations pane under **Systems > Provisioning > Directory**, for example phonebook@example.com, is used to provision users with one or more phone books that they have been given access to.

Phone book and access replication

Phone books and the access control defined for them are synchronized to the Cisco TMS Agent on Cisco TMS, which replicates to the Cisco TMS Agent on the VCS. Users searching with Movi or E20 will therefore get different phone book results depending on the user group they belong to.

Below is an illustration of how phone book data gets from Cisco TMS to the provisioned E20 or Movi client. Note that blue lines are relevant only to Movi, not E20.



Provisioning Source

After you install or upgrade Cisco TMS to version 12.6 or 13.0, Cisco TMS automatically creates a phone book source called Provisioning Source which includes all the users that you have created in the Directory Browser under **Systems > Provisioning > Directory**. You can verify the existence of this phone book source by going to **Phone Book > Manage Phone Book Sources**.

Note: If FindMe is not being used, and only the Device URI is being used in the Provisioning Directory, then the Provisioning Phone Book Source will not be populated until users begin to log into their devices whether this be a Movi client, E20 or both.

The main purpose of this phone book source is to give the Cisco TMS Administrator the possibility to create a Cisco TMS phone book using this phone book source, which in turn gives the Cisco TMS

Administrator the ability to 'set' this phone book on non-provisioned systems registered to the Cisco TMS.

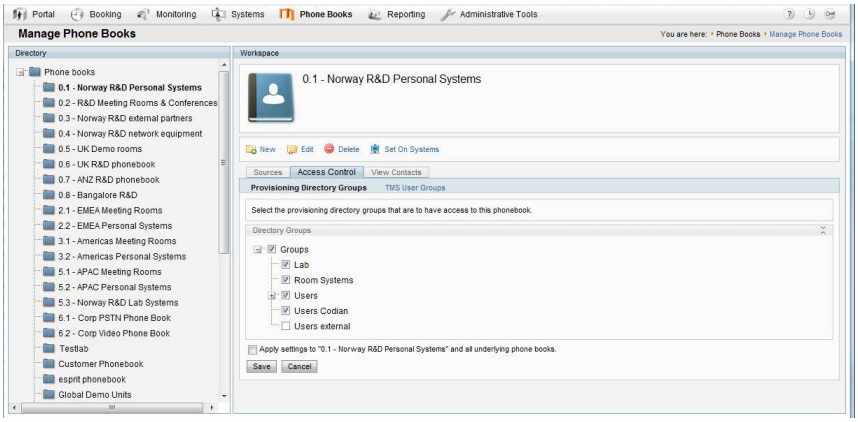
Note: When setting the phone book created from the Provisioning Source phone book source to an endpoint registered to the Cisco TMS, H.323-only endpoints registered to a Cisco VCS (or one of its cluster peers) will receive the SIP Alias Phone Book entries regardless of the endpoints not supporting SIP. The reason that this can occur is interworking on the Cisco VCS

Phone Book Sources Activity Status

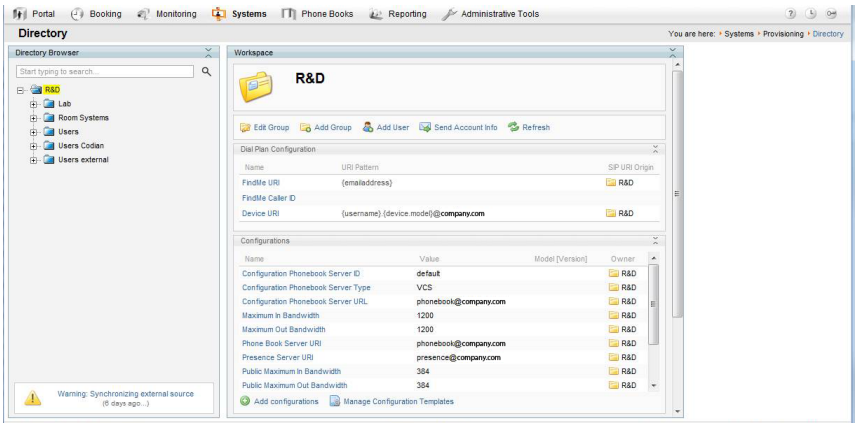
If necessary, you can monitor the activity status by going to **Phone Books > Phone Book Sources Activity Status** in Cisco TMS.

Setting access control

To provision a phone book to a user group, you must select the phone book in the **Directory** pane and go to the **Access Control** tab. From here you can select the user groups to be provisioned with that phone book. For example, in the picture below, the **Groups** selected with a check mark will have access to the **0.1 – Norway R&D Personal Systems**, while the group **Users external** will not.



As shown in the picture below, the **Groups** referred to on the **Access Control** tab are the same groups that you have built in the **Directory Browser** under **Systems > Provisioning > Directory**.



Diagnostics

In Cisco TMS, you can go to **Administrative Tools > TMS Agent Diagnostics** to monitor and schedule various diagnostic tests for the Cisco TMS Agents.

Cisco TMS Agent Diagnostics are run automatically after you have added your VCS(s) to the Cisco TMS and have enabled Cisco TMS Agent data replication on the Cisco VCS or Cisco VCS cluster. No configuration is required by the administrator. The diagnostic tests may also be scheduled for regular intervals and/or run manually at any time.

Note: For Cisco VCSs that have the Cisco TMS Agent installed, the Cisco TMS Agent Diagnostics pane is found by going to **Systems > Navigator > TMS Agent**.

Fixing problems uncovered by diagnostics

When problems are uncovered, a "Failed" icon will be displayed and details of the problem will be shown as well as instructions on how to fix the problem manually. In many cases, a button named **Fix** or **Set** will be displayed. Click the button to have the problem fixed automatically.

Scheduling diagnostics

In the **Schedule (Last run)** column under **Workspace** you can set the scheduled time for running the diagnostics at regular intervals.

1. Select option:
   - *None*
   - *Hourly*
   - *Daily*
   - *Weekly*
   - *Monthly*
   - or *default*, which is determined by parameters on the VCS.
2. Click **Save**.

Running the diagnostics

1. Start by selecting the Local Cisco TMS Agent or the Cisco VCS/VCS cluster you want to run diagnostics for in the Cisco TMS **Agent Browser** pane. If a Cisco VCS is in a cluster, expand **Clustered VCSs** from the tree view and then select the Cisco VCS.
2. Select the diagnostics you want to run from the **Workspace** pane. This pane shows a list of all diagnostics that can be run for a Cisco TMS Agent on a Cisco TMS server or Cisco VCS.
3. You can select all or some of these by clicking on **Check or Uncheck All** and then clicking on either the **Run Selected Diagnosis** or the **Run All Diagnosis** button.

For more details of the diagnostics that can be run, see the tables below. The details for each are displayed in Cisco TMS when clicking on each text under the **Diagnosis** column under the **Workspace** pane.

Local Cisco TMS Agent

Diagnosis	Description	Fix or set settings
Verify that the Cisco TMS Agent Diagnostics API is available and working properly.	If the diagnostics API is not available, further diagnostics is not possible.	Make sure that the Cisco TMS Agent Service is running and working properly.
Verify that all OpenDS database indexes are installed.	If the indexes are not installed it may cause slow OpenDS searches or missing phonebooks which can result in registered users not being found.	Clear the Enable Cisco TMS Agent Data Replication check box on the Cisco VCS in **System > Navigator** and re-enable data replication.
Verify that OpenDS database indexes are not degraded	If the indexes are degraded it may cause slow or faulty OpenDS searches, which may result in registered users not being found.	Click the **Fix** button to correct degraded indexes.
Verify that OpenDS is available.	If OpenDS is not available, the TMS will not function properly.	Two possible error messages: 1. Unable to communicate with OpenDS. Make sure that the Open DS windows service is running. Go to **Control Panel > Administrative Tools > Services**. 2. Could not authenticate with OpenDS. Contact Cisco support for more information.
Verify that all OpenDS database indexes are in a consistent state.	If the indexes are not in a consistent state it may cause slow or faulty OpenDS searches, which may result in registered users not being found.	Click the **Fix** button to rebuild the database indexes. **WARNING:** The Cisco TMS Agent will be unavailable while indexes are rebuilding.

Clustered Cisco VCSs

Diagnosis	Description	Fix or set settings
Verify that the Cisco TMS Agent Diagnostics API is available and working properly.	If the diagnostics API is not available, further diagnostics is not possible.	Make sure that the Cisco TMS Agent Service is running.
Verify that all OpenDS database indexes are installed.	If the indexes are not installed it may cause slow OpenDS searches or missing phonebooks which can result in registered users not being found.	Disable and re-enable replication. Go to the **Systems > Navigator > TMS Agent** tab. 1. Clear **Enable Cisco TMSAgent Data Replication**. 2. Click **Save Settings**. 3. Go back and select **Enable Cisco TMSAgent Data Replication**. 4. Click **Save Settings**.
Verify that the replication status, reported by OpenDS is normal.	If replication status is degraded, and this status remains the same over several hours, replication to this Cisco VCS needs to be disabled and then re-enabled again.	Disable and re-enable replication. Go to **Systems > Navigator > Cisco TMS Agent** tab. 1. Clear **Enable Cisco TMSAgent Data Replication**. 2. Click **Save Settings**. 3. Go back and select **Enable Cisco TMSAgent Data Replication**. 4. Click **Save Settings**.
Verify that OpenDS database indexes are not degraded	If the indexes are degraded it may cause slow or faulty OpenDS searches, which may result in registered users not being found.	Click the **Fix** button to correct degraded indexes.
Verify that the VCS has one or more subzones configured.	Subzones are set up for the purpose of bandwidth management. An Endpoints/Movi client that registers to a VCS is allocated to the appropriate subzone based on its IP address. If the endpoint's IP address does not match any of the subzones, it is assigned to the Default Subzone.	For more details, see section Zones and neighbors in the *Cisco VCS Administrator Guide*.
Verify that Calls to unknown IP addresses is set to "Indirect" on the VCS Control.	Calls to unknown IP addresses should be set to "Indirect" because the Cisco VCS Control will handle corporate internal calls only. The "Indirect" setting means that the Cisco VCS will query its neighbors for the remote address and if permitted will route the call through the neighbor.	Click the **Set** button to set **Calls to unknown IP addresses** to *Indirect*.

Verify that OpenDS is available.	If OpenDS is not available, the TMS Agent will not function properly.	Two possible error messages: 1. Unable to communicate with OpenDS. Make sure that the Open DS windows service is running. Go to **Control Panel > Administrative Tools > Services**. 2. Could not authenticate with OpenDS. Contact Cisco support for more information.
Verify that authentication is enabled on the Cisco TMS Agent.	If authentication is disabled, users will be provisioned by the Cisco TMS Agent without supplying a password.	To enable authentication, change the setting in **Administration tools > Configuration > TMS Agent Settings**.
Verify that the "Device Provisioning" option key is installed on the Cisco VCS Control.	See Installing option keys on the VCS for more information. If the "Device Provisioning" option key is not installed, provisioning will not work.	Contact Cisco to obtain the no-charge Device Provisioning option key.
Verify that SIP SIMPLE Presence User Agent is enabled on the Cisco VCS Control.	SIP SIMPLE Presence User Agent must be On and Active for the Cisco VCS to support publishing of presence status for endpoints that do not support presence.	The configuration must be identical for all VCSs in a cluster. For more information, see the section on Presence in the Cisco VCS Administrator Guide.
Verify that SIP Mode is enabled on the Cisco VCS Control.	Determines whether or not the Cisco VCS will provide SIP registrar and SIP proxy functionality. Note that SIP mode must be enabled in order to use either the Presence Server or the Presence User Agent.	Click the **Set** button to enable SIP Mode.
Verify that authentication is disabled on the Cisco VCS Control.	If authentication is enabled, clients will not be able to provisioned by the Cisco VCS Control - as the provisioning password is different to the registration authentication password.	Click the **Set** button to disable authentication.
Verify that SIP Routes are correctly configured.	SIP routes on Cisco VCSs are set up to handle routing of SIP (SUBSCRIBE) requests for endpoints/Movi clients registering to a Cisco VCS and (INFO) requests for phone book searches.	Click the **Set** button to resolve the problem.

Verify that all OpenDS database indexes are in a consistent state.	If the indexes are not in a consistent state it may cause slow or faulty OpenDS searches, which may result in registered users not being found.	Click the **Fix** button to rebuild the database indexes. **Warning:** The Cisco TMS Agent will be unavailable while indexes are rebuilding.
Verify that all host names in the replication domain can be resolved by doing DNS lookups.	If host names in the replication domain cannot be resolved, replication may fail.	Verify that the DNS settings on the Cisco VCS are correct and that the DNS server(s) specified are working properly.
Verify that SIP SIMPLE Presence Server is enabled on the VCS Control.	SIP SIMPLE Presence Server must be On and Active for processing of PUBLISH messages intended for the SIP domains for which the local Cisco VCS is authoritative. If peers have the Presence Server enabled, the Presence database is replicated across all peers in the cluster.	The configuration must be identical for all VCSs in a cluster. For more information, see the section on Presence in the Cisco VCS Administrator Guide.
Verify that Cisco VCS time doesn't deviate from the Cisco TMS time by more than 5 minutes.	When doing TLS encryption, the time deviation limit is 5 minutes. When the deviation is more than 5 minutes encryption will fail.	The current deviation is more than 3 minutes. Cisco recommends keeping time synchronized using a NTP (Network Time Protocol) server. If possible, both Cisco TMS and Cisco VCS should use the same NTP server. To set the NTP server for a Cisco VCS, navigate to **Settings > Edit Settings** tabs in the **Systems > Navigator** page. To set the NTP server for the Cisco TMS server, run the following command from a the command line: **`net time /setsntp:server_IP.`**
Verify that the Cisco VCS IP address is in the Local Cisco TMS Agent list of replicating agents.	If the Cisco VCS IP address isn't in the Local Cisco TMS Agent list of replicating agents, replication will fail.	Cisco TMS agent data replication is enabled for this Cisco TMS Agent, but the network address of this Cisco VCS was not found in the list of replicating agents read from the local agent. If you have recently enabled data replication for this system, wait and refresh after the background event on the Cisco TMS Server setting up the replication has finished. If not, try to re-enable the replication by turning if off and then back on again for this Cisco VCS in the **System Navigator > TMS Agent** tab.

Verify that the FindMe option key is present on the Cisco VCS when the FindMe option is enabled on the local Cisco TMS Agent	When the FindMe option is enabled and no FindMe option key is installed on the Cisco VCS, FindMe will not work correctly on the Cisco VCS in question. The User Policy option key needs to be installed. See Enable Device Provisioning on the Cisco VCS for more information on how option keys are added.	Contact Cisco to obtain this chargeable User Policy option key.
Verify that users created on the Local Cisco TMS Agent replicate to all the Cisco TMS Agent LDAP databases in the cluster.	Faulty replication leaves affected databases in an inconsistent state. Users and configuration will not be identical to master agent. As a result provisioning will fail.	Disable and re-enable replication. Go to **Systems > Navigator > TMS Agent** tab. 1. Clear **Enable Cisco TMSAgent Data Replication**. 2. Click **Save Settings**. 3. Go back and select **Enable Cisco TMSAgent Data Replication**. 4. Click **Save Settings**.
Verify that all VCS in a cluster have the same SIP domains.	The SIP domains that provisioned users shall register to must be present on all Cisco VCSs in a cluster for the users to be able to register.	To add a missing SIP domain to a Cisco VCS, go to **Configuration > Protocols >SIP > Domain**.

After starting diagnostics for all or some diagnosis, an "In queue" icon is displayed to the right of each diagnosis. After execution of each diagnosis a "Successful" or "Failed" icon will be displayed.

Reading the TMS Agent Diagnostics page

The **Cisco TMS Agent Browser** pane displays the Local Cisco TMS Agent, which is the agent running on the Cisco TMS server itself, as well as the agents running on each of the Cisco VCSs or Cisco VCS clusters that are added to Cisco TMS.

	Diagnosis shows that your provisioning process has a fatal error.
	Diagnosis has not yet been run.
	Diagnosis is complete and produced no warnings.
	Diagnosis shows that your provisioning process has an error but it is not critical.
	Diagnosis shows that there is a non-standard setting in Cisco TMS influencing the provisioning process.
	Diagnosis is pending/waiting/in queue.
	Diagnosis is running.

Monitoring diagnostics

When running these diagnostics, you will also find a "Run diagnostics on one specific Cisco TMS Agent" background job for each initiated diagnostic.

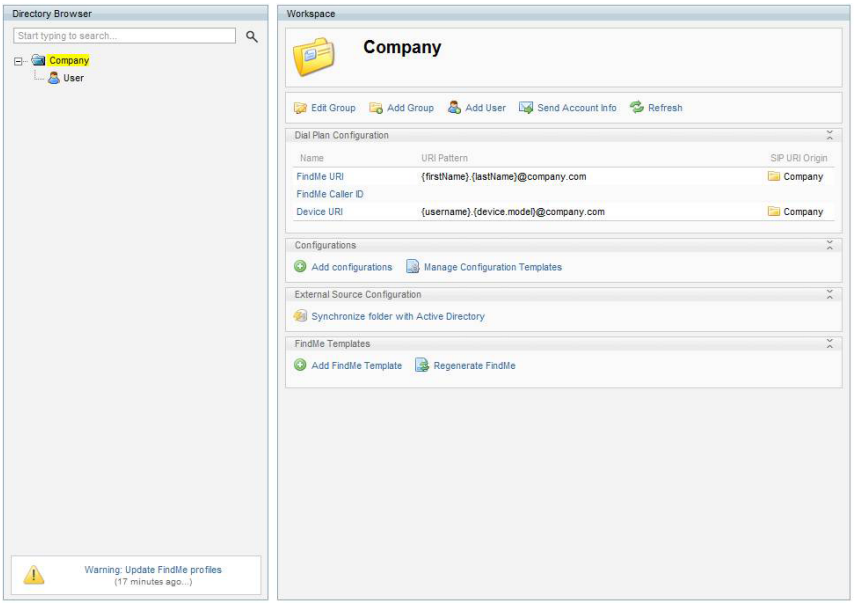
Go to **Administrative Tools > Activity Status** page to see the status of the diagnostics execution. If you enter this page before all tests are completed, you can click **Refresh** to get an up-to-date status.

Provisioning Directory Error Log

Some actions cannot be performed while scheduled procedures are running on Cisco TMS.

Some actions initiated from the GUI will cause specific scheduled job to execute asynchronously as a background job. Examples of such jobs are importing users from Active Directory and propagating FindMeURI's to the users in the Cisco TMS directory.

When an error occurs a warning will be displayed in the bottom left corner of the screen.

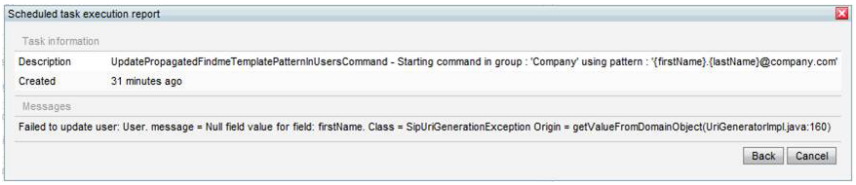


In this example the FindMe URI set on the group includes a property {firstName} which is not set on a user in the directory. Since the FindMe URI then cannot be generated, the error is logged in the application log and displayed as this warning.

To see a list of scheduled tasks for this warning, click the message in the box.

To see the technical details related to the warning, click the name of the message.

To delete a message, click the dropdown menu and select **Delete**.


Scheduled task execution report
Task information
Description
UpdatePropagatedFindmeTemplatePatternInUsersCommand - Starting command in group : 'Company' using pattern : '{firstName}.{lastName}@company.com'
Created
31 minutes ago
Messages
Failed to update user: User. message = Null field value for field: firstName. Class = SipUriGenerationException Origin = getValueFromDomainObject(UriGeneratorImpl.java:160)
Back
Cancel

Testing provisioning with Movi

This section describes how to quickly install and configure a Movi client for test purposes.

For general practice, Cisco recommends pre-configuring the Movi client before deployment to allow easy and swift use while reducing the potential user set-up mistakes to a minimum. Comprehensive information on the different methods to set and deploy the Movi client can be found in the deployment section of the *Cisco TelePresence Movi Administrator Guide*.

Obtaining Movi

When a new version of Movi is available, you see a Cisco TMS ticket if these two settings are enabled:

- **Administrative Tools > Configuration > Network Settings > Automatic Software Update**: **Automatically Check for Updates** is setto *Yes.*
- **Administrative Tools > Configuration > General Settings**: **Enable TMS Agents** is set to *Yes*.

The description field of the Cisco TMS ticket includes a link to download a zip file containing the setup files for Windows and Mac OS X, as well as a readme file describing the various setup file options.

Installing and configuring Movi

For a quick test that your Provisioning setup works for Movi on Windows, start by installing the .exe:

1. Run the MoviSetup.exe file to install Movi.
2. Upon launching the Movi client, you see the **Sign in** window.
3. Click the **Advanced** link, and complete the following fields.

- **Internal VCS**: The DNS address of the internal VCS cluster.
- **External VCS**: The DNS address of the VCS Expressway cluster.
- **Domain**: Identical to the SIP domain configured on the VCS. (In VCS, go to **VCS configuration > Protocols > SIP > Domains**).

4. Click **OK** to return to the **Sign in** window.

Verifying that provisioning works

Now sign in and make sure Movi receives provisioning data:

1. Enter the username and password of the test account you have created. (See Create and manage user accounts.) Click **Sign in**.
2. Verify that you can make and receive calls.
3. Check that the phone books provisioned to your user can be accessed as expected.
4. Verify that you are able to change and publish your presence status using Movi.

Note: To troubleshoot issues that may arise, refer to the Provisioning troubleshooting guide and Diagnostics in this document.

DNS setup for provisioning E20

This section describes the DNS setup necessary for provisioning E20 outside the firewall.

In standard Cisco VCS/Cisco TMS deployments for enterprises, some endpoints are connected to the intranet while others are connected to a variety of home networks outside the firewall. In the latter case, the E20 needs to connect to the Cisco VCS/Cisco TMS infrastructure through a Cisco VCS Expressway located outside the company firewall. Consequently, the E20 must be provisioned with a Cisco VCS Expressway as the SIP proxy. This is only possible if the external manager entered into the E20 wizard is resolved through DNS.

If provisioning is done internally, this setup is optional; however, it will allow for a flexible failover/load-balancing scheme for the Cisco VCS cluster.

NAPTR records

A Name Authority Pointer (NAPTR) record is a DNS record used for regular expression rewrite rules for domain names.

Setting up these DNS entries can be done in two ways. The DNS infrastructure could return different NAPTR records depending on whether the external manager is located inside or outside the firewall. If this is not possible, the DNS names of the external manager addresses must be different and resolve to two different NAPTR records on the same DNS server.

Flags

The E20 bases its provisioning request on the NAPTR record flag:

- "s" indicates that the NAPTR response is an SRV record. If the flag is "s" only, the E20 will be provisioned from the internal Cisco VCS.
- "e" indicates that the SIP proxy is located outside the firewall (e=external). This indicator is Cisco proprietary. If the flag is "se", the E20 will be provisioned from the external Cisco VCS.

Required NAPTR record for external endpoint provisioning

For an encrypted TCP connection, use the following type of record to point to the SIP secure service:

```
example.com. IN NAPTR 50  50 "se" "SIPS+D2T" "" _sips._
tcp.example.com.
```

For a non-encrypted TCP connection, use the following type of record to point to the TCP SIP service:

```
example.com. IN NAPTR 90  50 "se" "SIP+D2T" "" _sip._
tcp.example.com.
```

For a non-encrypted UDP connection, use the following type of record to point to the TCP SIP service:

```
example.com. IN NAPTR 100 50 "se" "SIP+D2U" "" _sip._
udp.example.com.
```

Optional NAPTR record for internal endpoint provisioning

For an encrypted TCP connection, use the following type of record to point to the SIP secure service:

```
example.com. IN NAPTR 50  50 "s" "SIPS+D2T" "" _sips._
tcp.example.com.
```

For an unencrypted TCP connection, use the following type of record to point to the TCP SIP service:

```
example.com. IN NAPTR 90  50 "s" "SIP+D2T" "" _sip._
tcp.example.com.
```

For a unencrypted UDP connection, use the following type of record to point to the TCP SIP service:

```
example.com. IN NAPTR 100 50 "s" "SIP+D2U" "" _sip._
udp.example.com.
```

SRV records

An SRV record or Service record is used to indicate the location, priority and weight of a service, in this case the Cisco VCS. SRV records can offer load-balancing capabilities to an E20/VCS/Cisco TMS deployment.

SRV records for external endpoint provisioning

The SRV record points to the port number and the A record (see below) of the provisioning server.

For encrypted TCP:

```
_sips._tcp.example.com. IN SRV 0 1 5061 vcs.example.com.
```

For unencrypted TCP:.

```
_sip._tcp.exmple.com. IN SRV 0 1 5060 vcs.example.com.
```

For unencrypted UDP:

```
_sip._udp.example.com. IN SRV 0 1 5060 vcs.example.com.
```

A records

An A record or Address record is used to map a hostname to an IP address. In addition to NAPTR and SRV records, the DNS server must also be configured with one A record for each provisioning server.

Based on the above SRV examples, the A record of the provisioning server that the SRV record points to should be:

```
vcs IN A <ip address of the provisioning server>
```

Verifying the DNS records

To verify that your DNS records are set up and work as expected, use the tool nslookup or similar. Type, for example:

```
nslookup -querytype=srv _sip._udp.example.com
```

and then check the output.

Testing provisioning with E20

To make the provisioning scheme work, the E20 endpoint must be set up with a username, password, domain, and external manager address. These parameters can be entered into the provisioning wizard of the E20 during the first startup of the device:

Configuring the endpoint

1. Connect the E20 to a LAN.
2. Go to **Settings > Configure your E20**.
3. Enter the username and password you have created. (See Create and manage user accounts.)
4. The Domain should be identical to the SIP domain configured on the Cisco VCS.
5. Enter the Cisco VCS address as External Manager. Press **OK**.

Verifying that provisioning works

The E20 should now sign in and register. Make sure provisioning data has been received:

1. Verify that the endpoint's URI is visible in the top left corner of the screen.
2. Verify that you can make and receive calls.
3. Check that the phone books provisioned to your user is available on the endpoint.

Note: To troubleshoot issues that may arise, refer to the section Diagnostics in this document, and to the *Cisco TMS Provisioning Troubleshooting Guide* document.

Removing provisioning from a VCS

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

On the Cisco VCS:

1. Go to **Maintenance > Option keys**.
2. Select the **Device Provisioning** option key.
3. Click **Delete**.
4. Log in to the VCS command line interface
5. Type: **`xconfiguration SIP Routes`**.

This will provide a list of SIP route entries. If Device Provisioning is not enabled, there should be no SIP route entries, so if there are any, these need to be deleted:

1. Find the number after the words "SIP Routes Route" for each entry.
2. For each different number in the SIP Routes entries, type **`xcommand SipRouteDelete SipRouteID`**: <number>
3. Once all <number> entries have been deleted, confirm that all the SIP routes have been deleted by doing the following:
   a. Type: **`xconfiguration SIP Routes`**
   b. Check that Cisco VCS reports *OK* with no SIP Route information.

Related documents

When configuring provisioning for the first time, having comprehensive documentation at hand will be helpful. You can find these, and other relevant documents, on our website at http://www.tandberg.com/support/video-conferencing-documentation.jsp.

Document title	Reference number
Cisco TMS Administrator Guide	D13741
Cisco VCS Administrator Guide	D14049
Cisco VCS Cluster Creation and Maintenance Deployment Guide	D14367
Cisco VCS FindMe Deployment Guide	D14525
Cisco TMS Installation and Getting Started Guide	D14389
Cisco TelePresence Movi Administrator Guide	D14410
Cisco TelePresence System E20 Administrator Guide	D14330
Cisco TMS Provisioning Troubleshooting Guide	D14427

Checking for updates and getting help

We recommend registering your product at http://www.tandberg.com/services/video-conferencing-product-registration.jsp in order to receive notifications about the latest software and security updates. New feature and maintenance releases are published regularly, and we recommend that your software is always kept up to date.

If you experience any problems when configuring or using the product, consult the documentation at http://www.tandberg.com/support/video-conferencing-documentation.jsp for an explanation of how its individual features and settings work. You can also check the support site at http://www.tandberg.com/support/ to make sure you are running the latest software version.

You or your reseller can also get help from our support team by raising a case at http://www.tandberg.com/support/. Make sure you have the following information ready:

- The software build number which can be found in the product user interface (if applicable).
- Your contact email address or telephone number.
- The serial number of the hardware unit (if applicable).

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

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

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

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

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

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