Cisco TelePresence Management Suite Agent Legacy

Deployment Guide

Cisco TMS 13.2
Cisco VCS X7.0/X7.1

D14368 07

August 2013

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 Cisco TMS Provisioning User Directory and Provisioning information from Cisco TMS via a single or clustered Cisco VCSs to endpoint devices such as Cisco Jabber Video for TelePresence, Cisco TelePresence System EX90 and Cisco IP Video Phone E20.

Cisco TMS Agent Legacy versus Cisco TelePresence Management Suite Provisioning Extension

This document describes provisioning using Cisco TelePresence Management Suite Agent Legacy, which is included in Cisco TMS version 13.2 and earlier.

We recommend that new users install and deploy Cisco TelePresence Management Suite Provisioning Extension (Cisco TMSPE), which is a new extension product supported by Cisco TMS version 13.2 and later. See *Cisco TelePresence Management Suite Provisioning Extension Deployment Guide* for instructions.

This guide

The table of contents indicates the sequence to take when planning and implementing a simplified provisioning deployment.

Since provisioning builds upon existing capabilities in Cisco TMS and Cisco VCS, 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.

Prerequisites and recommendations

This section describes prerequisites and best practices for deployment.

Cisco TMS requirements

Product	Version/description
Cisco TMS	13.2
Cisco TelePresence Movi 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.

Access to executing *.cmd and *.bat

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 Cisco TMS server during installation and upgrades.

Cisco TelePresence Management Server

If using the legacy product Cisco TelePresence Management Server, we recommend the Provisioning Directory be limited to a maximum of 5000 users.

Ports used by Cisco TMS Agent Legacy

Cisco TMS Agent Legacy uses the following ports:

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

Cisco VCS requirements

Product	Version/description
Cisco VCS	X7.0 or X7.1
Device Provisioning option key	Obtain free of charge from Cisco.
FindMe option key	Purchase separately from Cisco.

Clustering

Each VCS can support up to 2500 video client registrations (a combination of Jabber Video clients and any other compatible H.323/SIP endpoints or infrastructure). Up to six Cisco VCS peers can be combined in a single cluster, supporting a maximum of 10,000 video client registrations (the fifth and sixth peers in the cluster provide resilience 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 for your version.

DNS resolution for all devices

An IP address and a DNS name are needed for:

- Each Cisco VCS
- The Cisco TMS server

Make sure these DNS names resolve to the proper IP addresses before following the procedures in 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.

For instructions on setting up the Cisco VCS cluster name and DNS SRV records, see *Cisco TelePresence Video Communication Server Cluster Creation and Maintenance Deployment Guide*.

SMTP server

For Cisco TMS to be able to email 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. If your SMTP server requires authentication, make sure you have this information available before starting.

Best practices for deployment

Synchronizing time in Cisco VCS and Cisco TMS

We recommend keeping time synchronized using an NTP (Network Time Protocol) server. If possible, both Cisco TMS and Cisco VCS must 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 the Microsoft support article *How to configure an authoritative time server in Windows Server*. To configure the NTP server on the Cisco VCS, go to **System > Time**.

Active Directory

We recommend using Microsoft Active Directory to automate the creation and management of users. You will 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.

Enabling Cisco TMS Agent Legacy

Cisco TMS Agent Legacy is disabled by default in new installations of Cisco TMS.

To enable:

1. Go to **Administrative Tools > Configuration > General Settings**
2. Set **Enable Cisco TMS Agents** to *Yes*.
3. Go to **Administrative Tools > TMS Agent Diagnostics**.
4. Click **Run All Diagnoses**
   - If all check marks are green, proceed to Configuring Cisco VCS for provisioning [p.9].
   - If any diagnostic tests show errors, see Diagnostics [p.41]. All errors must be resolved before proceeding with setting up Cisco TMS and Cisco VCS for provisioning.

Configuring Cisco VCS for provisioning

This section describes how to configure Cisco VCS to work with Cisco TMS Agent Legacy.

Provisioning within your network

There are two types of Cisco VCS:

- **Cisco 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 .
- **Cisco 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 Cisco VCS Expressways, you can configure your system with provisioning enabled on the Cisco 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 Cisco VCS Expressways and Cisco VCS Controls (where some endpoints - such as soft clients - may register to either the Control or the Expressway), we recommend that you configure and enable provisioning only on the Cisco VCS Control (or Control cluster). If a soft client or other endpoint registers to a Cisco VCS Expressway, provisioning requests will be routed (using search rules) to the Cisco VCS Control associated with the 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 Cisco VCS (Control or 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.53].

Setting up DNS for the Cisco VCS

Cisco VCS must use DNS and be addressable via DNS. To configure the 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 > System**, 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**.

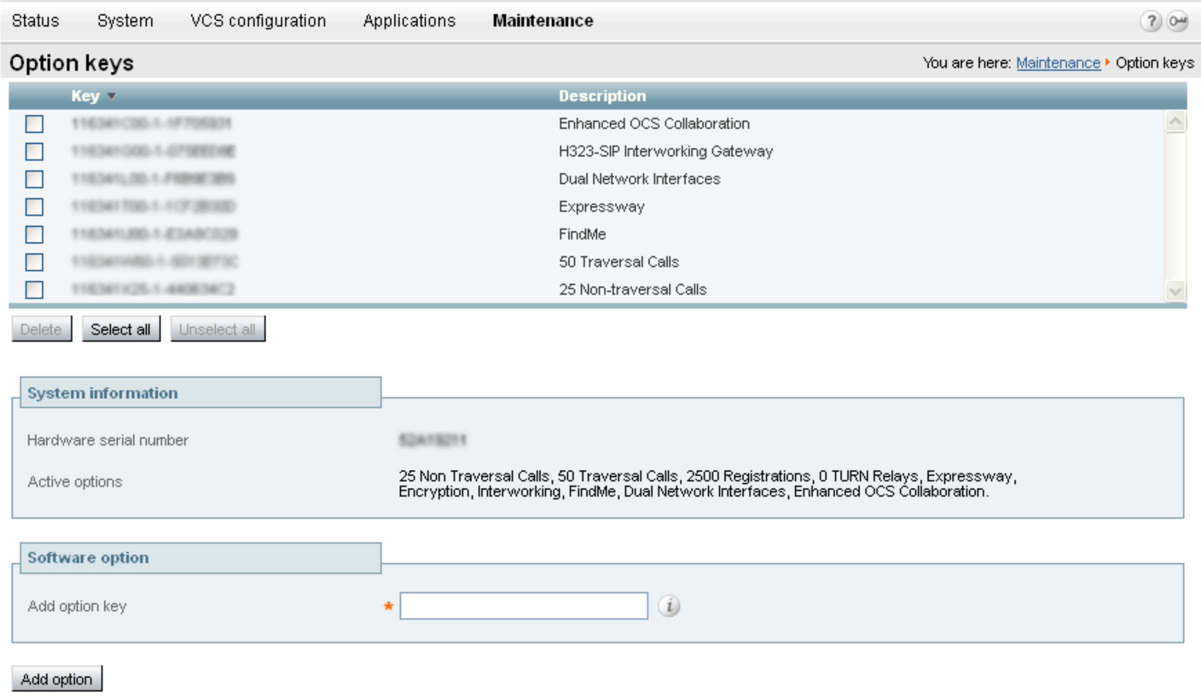
Installing the Device Provisioning option key

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 VCS, and must be identical on all 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**.



	Key	Description
□	[redacted]	Enhanced OCS Collaboration
□	[redacted]	H323-SIP Interworking Gateway
□	[redacted]	Dual Network Interfaces
□	[redacted]	Expressway
□	[redacted]	FindMe
□	[redacted]	50 Traversal Calls
□	[redacted]	25 Non-traversal Calls

System information

Hardware serial number: [redacted]

Active options: 25 Non Traversal Calls, 50 Traversal Calls, 2500 Registrations, 0 TURN Relays, Expressway, Encryption, Interworking, FindMe, Dual Network Interfaces, Enhanced OCS Collaboration.

Software option

Add option key *

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 Cisco VCS Event Log, immediately after enabling device provisioning, you will see

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

Enabling SIP

SIP must be enabled on each Cisco VCS (Controls and Expressways) in the network:

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

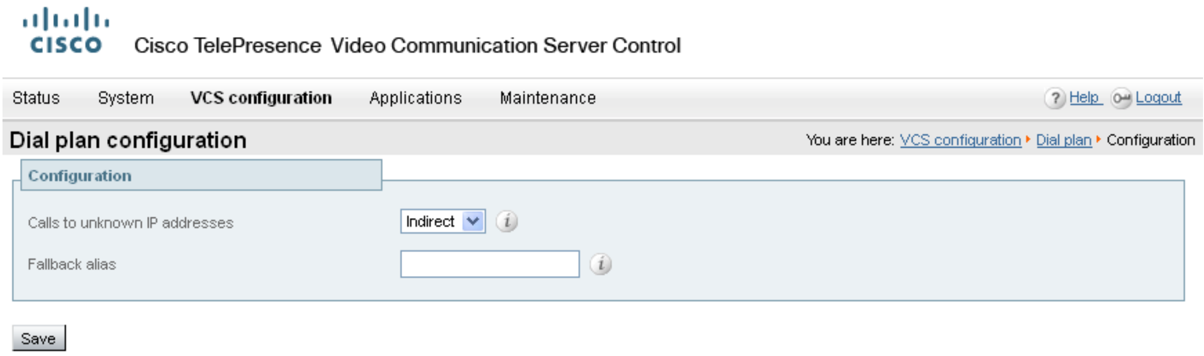
Configuring how Cisco VCS handles calls to unknown IP addresses

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 (**VCS configuration > Dial plan > Configuration**).

Cisco VCS Control

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



Dial plan configuration

You are here: VCS configuration ▸ Dial plan ▸ Configuration

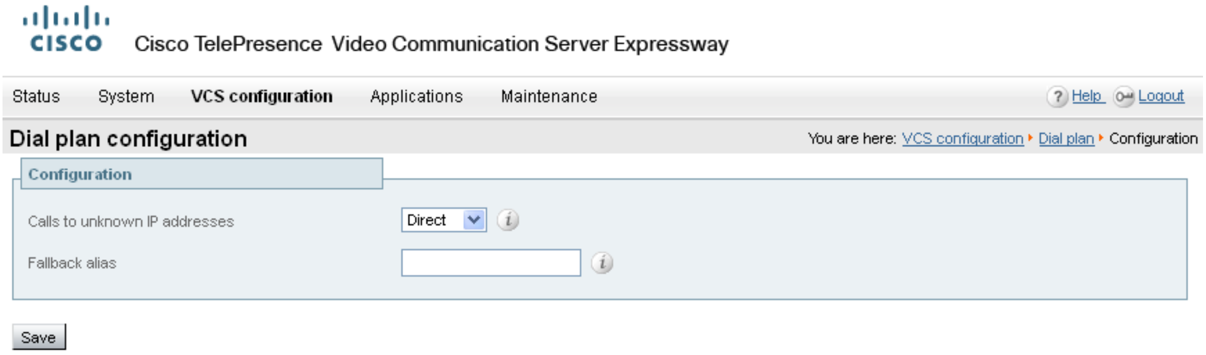
Configuration

Calls to unknown IP addresses: Indirect

Fallback alias:

Cisco VCS Expressway

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



Dial plan configuration

You are here: VCS configuration ▸ Dial plan ▸ Configuration

Configuration

Calls to unknown IP addresses: Direct

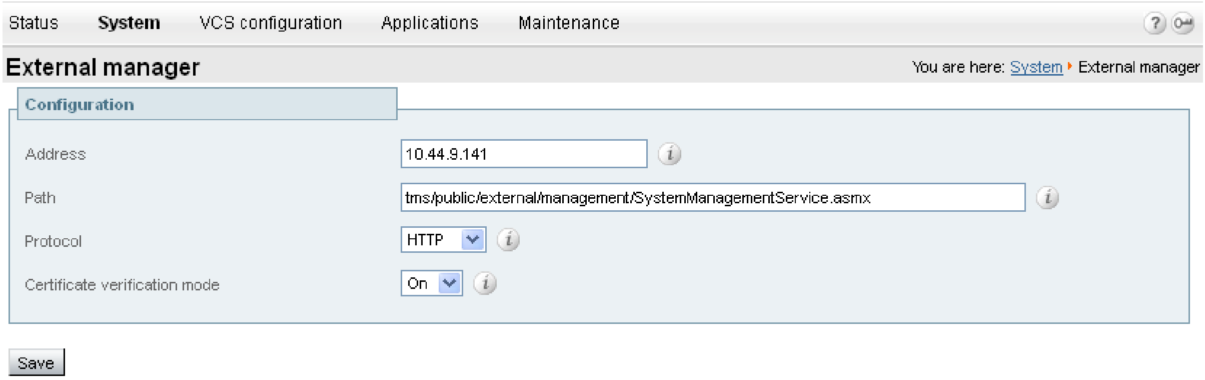
Fallback alias:

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 Cisco VCS Control), and optional for other Cisco VCSs (a Cisco 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 Cisco 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**.

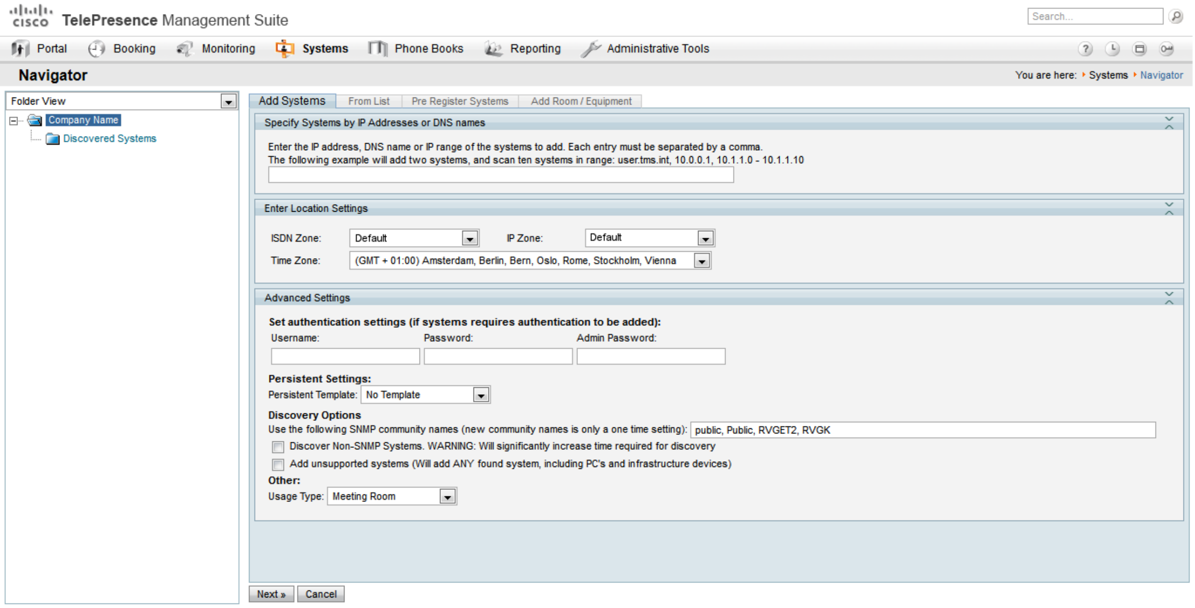


Address	10.44.9.141
Path	tms/public/external/management/SystemManagementService.asmx
Protocol	HTTP
Certificate verification mode	On

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.



Specify Systems by IP Addresses or DNS names

Enter the IP address, DNS name or IP range of the systems to add. Each entry must be separated by a comma.
The following example will add two systems, and scan ten systems in range: user.tms.int, 10.0.0.1, 10.1.1.0 - 10.1.1.10

Enter Location Settings

ISDN Zone: Default
IP Zone: Default
Time Zone: (GMT + 01:00) Amsterdam, Berlin, Bern, Oslo, Rome, Stockholm, Vienna

Advanced Settings

Set authentication settings (if systems requires authentication to be added):
Username:
Password:
Admin Password:

Persistent Settings:
Persistent Template: No Template

Discovery Options
Use the following SNMP community names (new community names is only a one time setting): public, Public, RVGET2, RVGK
□ Discover Non-SNMP Systems. WARNING: Will significantly increase time required for discovery
□ Add unsupported systems (Will add ANY found system, including PC's and infrastructure devices)

Other:
Usage Type: Meeting Room

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

If you are going to use FindMe, you must set the Cisco VCS 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 Cisco VCS cluster 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 VCS, for example "vcs1.example.com".
3. Click **Save**.
4. If there is any existing FindMe data, it must be updated to use the new cluster name:
   - Use the **`transferfindmeaccounts`** script to update the FindMe data to use this new name, using the process defined in *Cisco VCS Cluster Creation and Maintenance Deployment Guide*.

Turn on provisioning (enable TMS Agent data replication)

Cisco VCS is not part of a cluster

To turn on provisioning on a Cisco VCS that is not part of a cluster:

1. In Cisco TMS, go to **Systems > Navigator > Folder View.**
2. Select the Cisco VCS. This displays the device page.
3. Select the **TMS Agent** tab.
4. Click **Enable TMS Agent Data Replication**. This may take a while to complete (approximately 5 minutes, see note on **Activity Status** below).
5. Click **Save**.

In Cisco TMS, go to **Administrative Tools > Activity Status** to see activities that are active, scheduled or in progress in Cisco TMS. 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 Cisco VCS. 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**.

Enabling authentication (recommended)

Enabling authentication means that a password is required to access the database that stores the provisioning information.

This is enabled in two places in Cisco TMS. Cisco TMS then makes sure that the connected Cisco VCSs are configured with the relevant details.

In Cisco TMS:

1. Go to **Administrative Tools > Configuration > TMS Agent Settings**.
2. In the **Global (applied to all agents)** pane, ensure that **Authentication Enabled** is set to *Yes*.
3. Click **Save**.
4. For each Cisco VCS:
   1. Go to **Systems > Navigator > Folder View**.
   2. Select the Cisco VCS.
   3. Select the **TMS Agent** tab.
   4. Ensure that **Enable TMS Agent Data Replication** is selected.
   5. 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 Cisco 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**

We recommend that the **LDAP Configuration Password** and **LDAP Replication Password** be different. Ensure that these passwords are noted and secured appropriately.

Checking 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 > TMS Agent Diagnostics > TMS Agent** tab.
- From the same location you can access the **Cisco TMS Agent Diagnostics** by selecting the **Cisco TMS Agent Diagnostics** link located next to the **Cisco TMS Agent Configuration** link at the top of the tab.

On Cisco VCS:

- You can view the Cisco TMS Agent replication status by selecting the link **View Cisco TMS Agent replication status** on the **VCS configuration > Clustering** page.

See Running the diagnostics [p.41] for more information concerning Cisco TMS Agent Diagnostics.

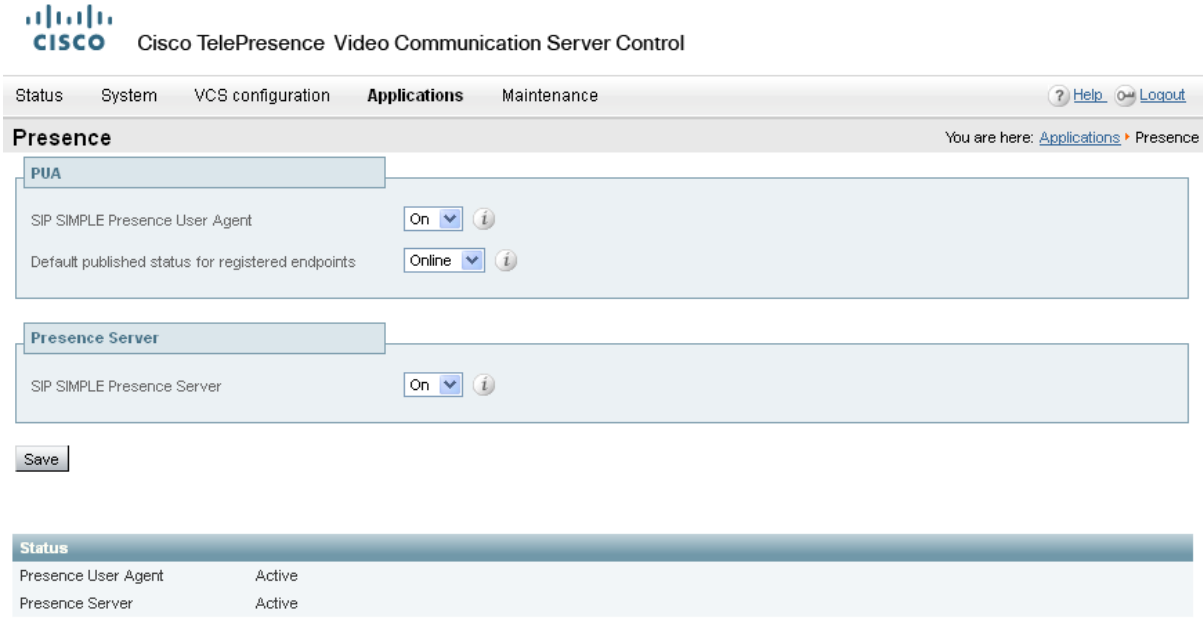
Enabling Presence on the Cisco VCS

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 Cisco VCS Control **Applications > Presence** set **SIP SIMPLE Presence Server** to *On*.
2. If Cisco 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*.


Cisco TelePresence Video Communication Server Control
Status
System
VCS configuration
Applications
Maintenance
Help
Logout
You are here: Applications ▸ Presence
Save

Presence

PUA

SIP SIMPLE Presence User Agent	On
Default published status for registered endpoints	Online

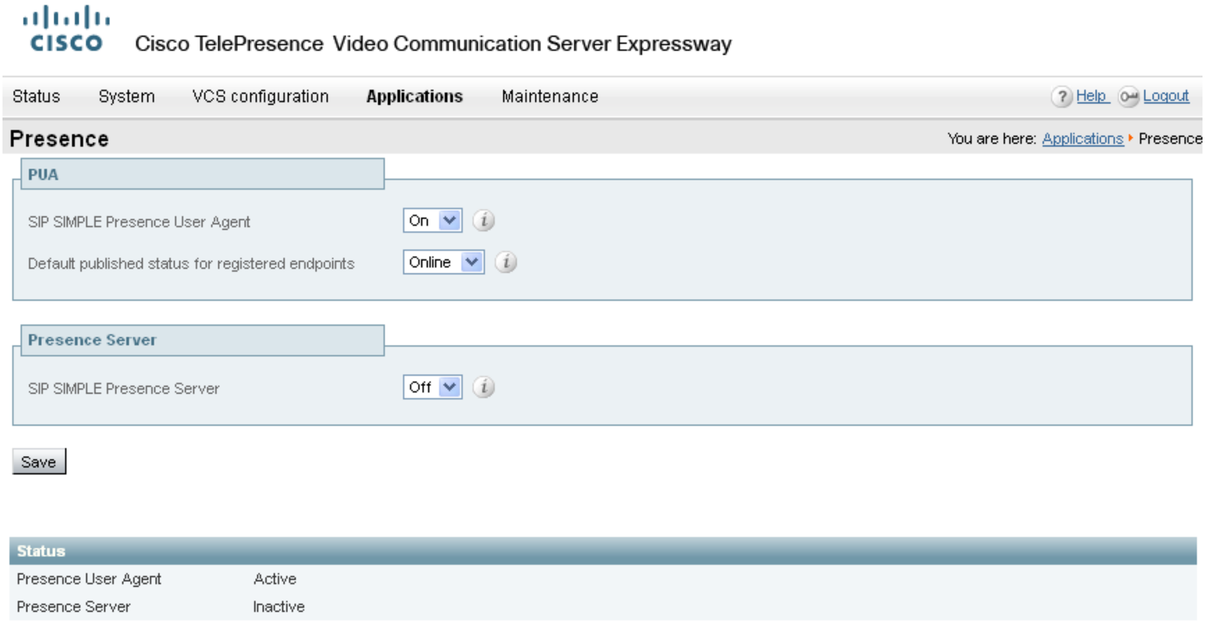
Presence Server

SIP SIMPLE Presence Server	On

Status	
Presence User Agent	Active
Presence Server	Active

Presence on Cisco VCS Expressway

1. In Cisco VCS Expressway **Applications > Presence** set **SIP SIMPLE Presence Server** to *Off*.
   The Presence Server must not be enabled on Cisco VCS Expressway; Cisco VCS Expressway must pass presence information to the Presence Server on Cisco VCS Control rather than keep the presence information locally.
2. If Cisco 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*.



Cisco TelePresence Video Communication Server Expressway
Status
System
VCS configuration
Applications
Maintenance
Help
Logout

Presence

You are here: Applications ▸ Presence

PUA

SIP SIMPLE Presence User Agent: On

Default published status for registered endpoints: Online

Presence Server

SIP SIMPLE Presence Server: Off

Status	
Presence User Agent	Active
Presence Server	Inactive

Setting up and maintaining the Provisioning Directory

This section describes how to set up, maintain, and configure a directory of provisioning users.

Note that while there is no hard limitation on number of users in the provisioning directory, a Cisco VCS cluster will support up to 10 000 users.

Overview of the Provisioning Directory

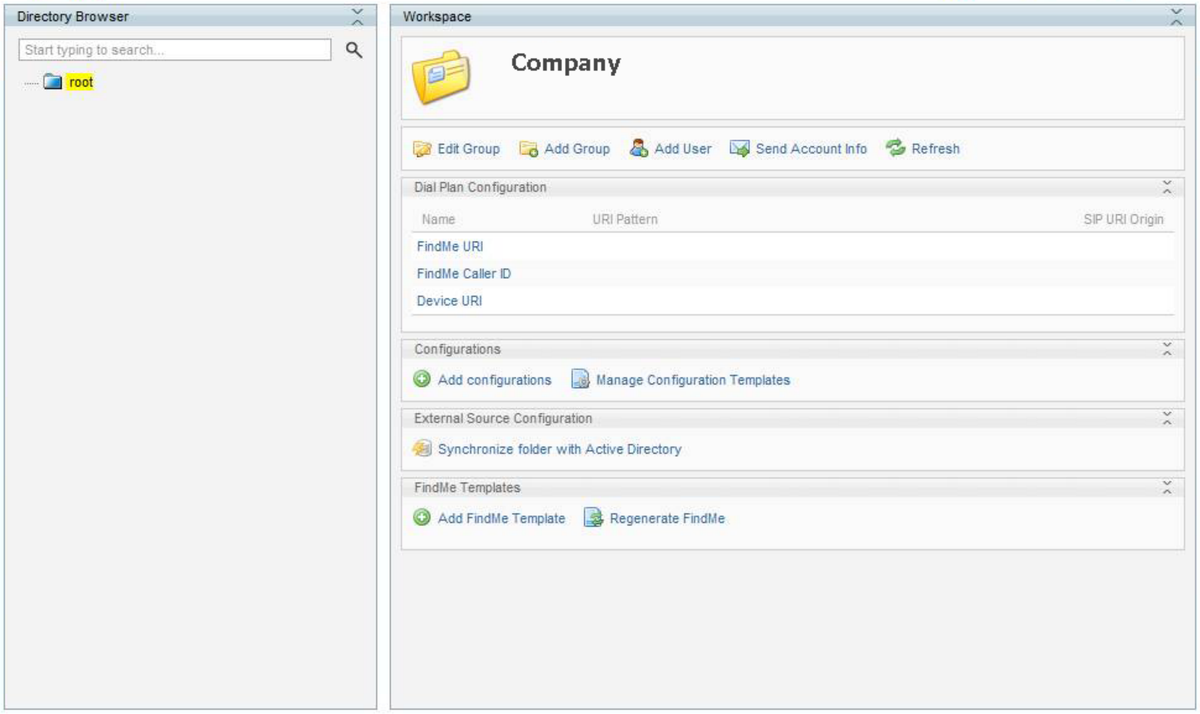
The Provisioning directory is located in Cisco TMS at **Systems > Provisioning > Directory**.

- 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.

Which panes and functions are available depends on your current location in the directory structure as well as which services are enabled:

- 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 see the **Devices** subsection pane, showing the user's provisioned devices.
- FindMe will not be seen if FindMe is disabled in **Administrative Tools > Configuration > Cisco TMS Agents Settings**. FindMe is enabled by default.

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 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.

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.

See Configuring a dial plan [p.29] for guidance on setting this up.

Configurations pane

In the **Configurations** pane, you set up and manage the configurations that endpoints will receive on provisioning.

Before configuration, templates that match the types and versions of endpoints in your deployment must be uploaded. See Uploading a new configuration template [p.30].

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. We recommend utilizing AD to import users. See Using Microsoft Active Directory for automated user creation and maintenance (recommended) [p.20].

FindMe Templates pane

In the **FindMe Templates** pane, the administrator can 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.

Using Microsoft Active Directory for automated user creation and maintenance (recommended)

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

Users imported to the User Directory in Cisco TMS will have icons with gray shirts, while manually created users will have blue shirts. For information concerning the manual creation of users, see the section Manual user creation and management (optional) [p.24].

Synchronizing with AD

After initial configuration and synchronization, the User Directory will automatically synchronize with Active Directory once a day. The time of the update is displayed on screen.

Note that only usernames and those fields shown in Mapping of user fields [p.31] are synchronized—the user's AD password is *not* imported into the User Directory. A provisioning password for each user will be automatically assigned.

Currently, the automatic synchronization cannot be changed, but you can run the AD synchronization manually at any time. We recommend running manual synchronizations at the highest group folder level possible according to your External Source Configuration plan.

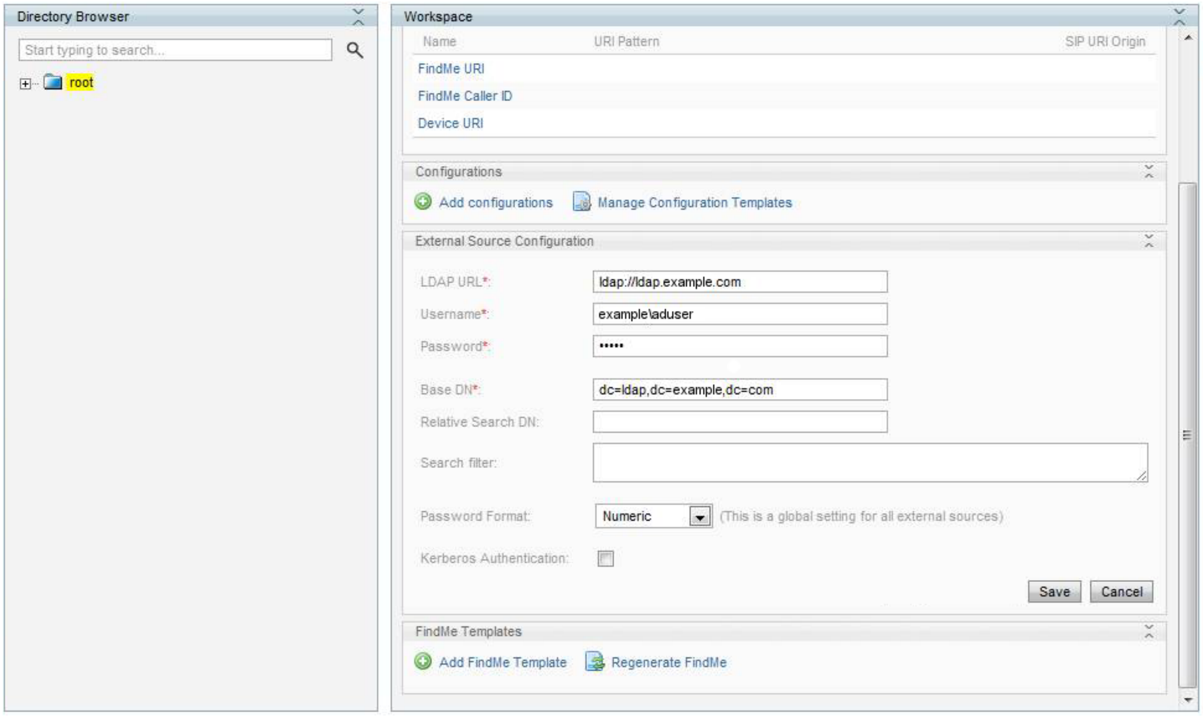
For example, if your External Source Configuration begins importing users at root and you have created search filters that place users in sub group folders under root, then you should run the manual synchronization from root. You can also run a manual synchronization at the sub group folder level, but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

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

Note: Cisco TMS Agent Legacy does not support the following characters are not allowed in usernames or display names: `\,+"<>./`. Importing names that contains these characters may lead to issues with for example phone book parsing.

Synchronizing from root level

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://globalcatalog.company.int:3268`.
4. Enter the **Username** to use when logging on and importing from Active Directory. We recommend 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**.



Name	URI Pattern	SIP URI Origin
FindMe URI		
FindMe Caller ID		
Device URI		

LDAP URL*: ldap://ldap.example.com

Username*: example\aduser

Password*: •••••

Base DN*: dc=ldap,dc=example,dc=com

Relative Search DN:

Search filter:

Password Format: Numeric (This is a global setting for all external sources)

Kerberos Authentication: □

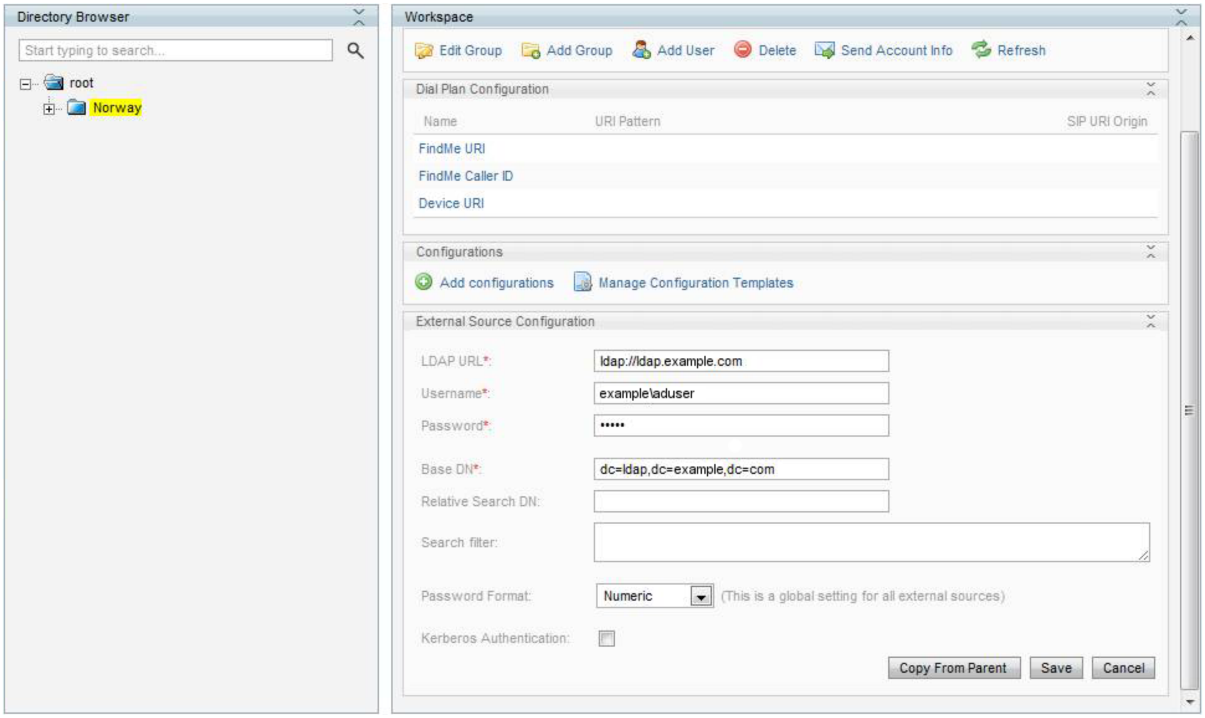
To import users immediately:

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.

Managing synchronization 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)



LDAP URL*: ldap://ldap.example.com

Username*: example\aduser

Password*: •••••

Base DN*: dc=ldap,dc=example,dc=com

Relative Search DN:

Search filter:

Password Format: Numeric (This is a global setting for all external sources)

Kerberos Authentication: □

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**.

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 window.

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.

Security groups and distribution lists

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, if you need to search on a security group in AD, enter the **Base DN** (such as **`dc=eu, dc=company, dc=com`**), leave the **Relative Search DN** blank, and enter your search in the **Search filter**, for example **memberOf= cn=videoconfusers, ou=security groups, dc=subdomain, dc=domain**.

Kerberos authentication

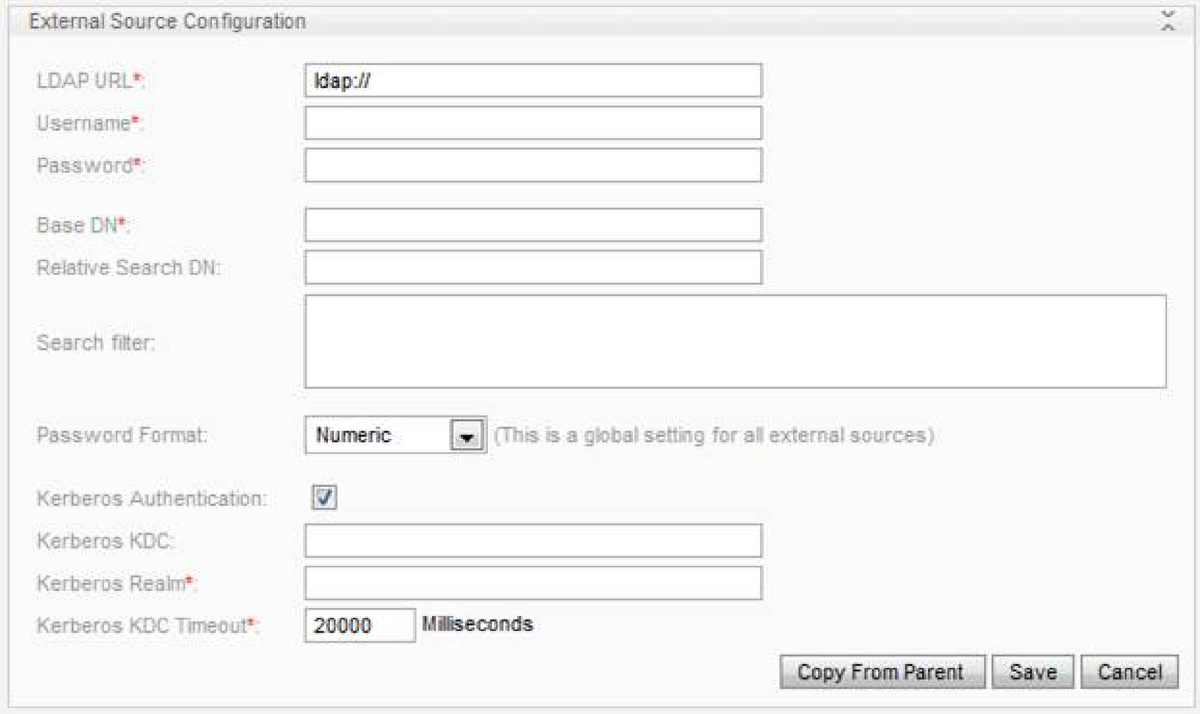
To import users using a secure connection, Cisco TMS supports Kerberos authentication towards AD. Note that this security only applies to the connection with Active Directory; it does not set up users to use Kerberos authentication for provisioning.

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

1. Click the **Edit** button.
2. Check **Kerberos Authentication** 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.



External Source Configuration

LDAP URL*: ldap://
Username*:
Password*:
Base DN*:
Relative Search DN:
Search filter:
Password Format: Numeric (This is a global setting for all external sources)
Kerberos Authentication: ☑
Kerberos KDC:
Kerberos Realm*:
Kerberos KDC Timeout*: 20000 Milliseconds

Manual user creation and management (optional)

While we strongly recommend the use of 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.
   Note that the following characters are not allowed in usernames or display names: `\,+"<>./`.
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. We recommend allowing Cisco TMS to generate these IDs, as they should be unique to each user.

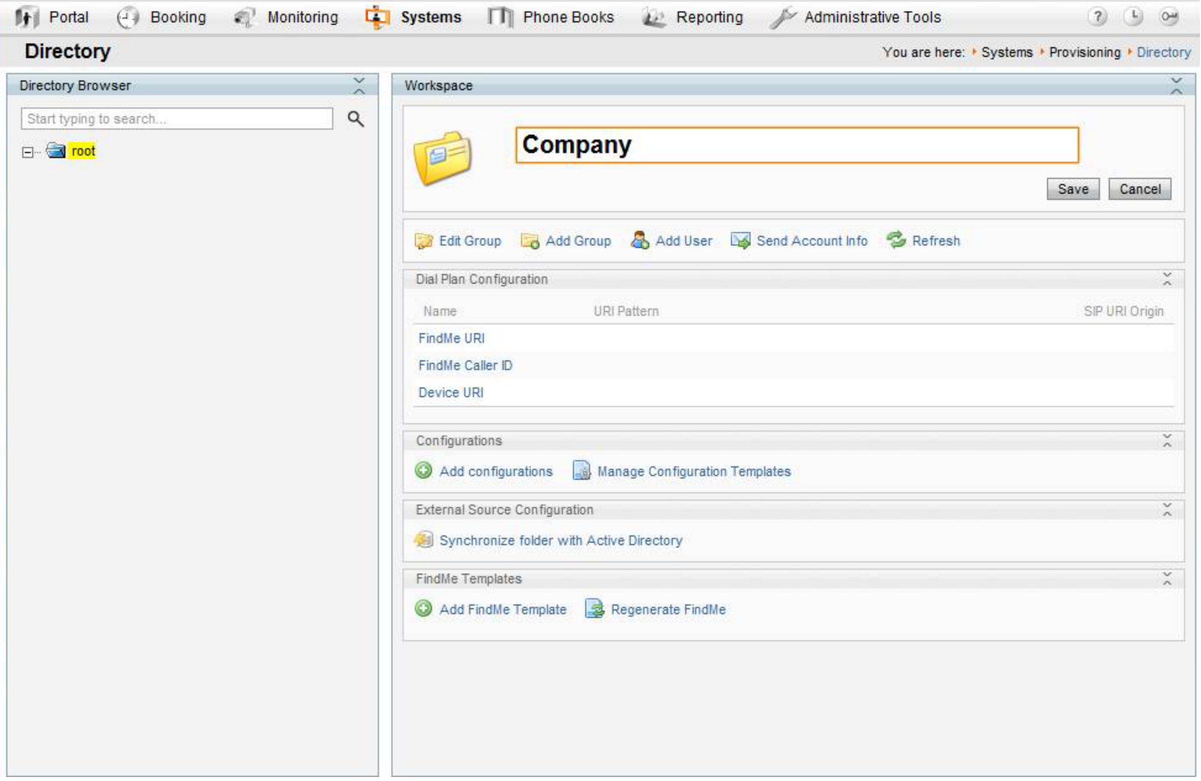
This finalizes the provisioning setup in Cisco TMS. The settings that were configured during this process will now be replicated to the Cisco VCS or cluster of VCSs by the Cisco TMS Agent. Any future configuration changes made in the Provisioning Directory UI in Cisco TMS will be replicated to the Cisco VCS or cluster of 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 provisioning deployment using Jabber Video and E20.

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:



Company

Dial Plan Configuration

Name	URI Pattern	SIP URI Origin
FindMe URI		
FindMe Caller ID		
Device URI		

Configurations

Add configurations   Manage Configuration Templates

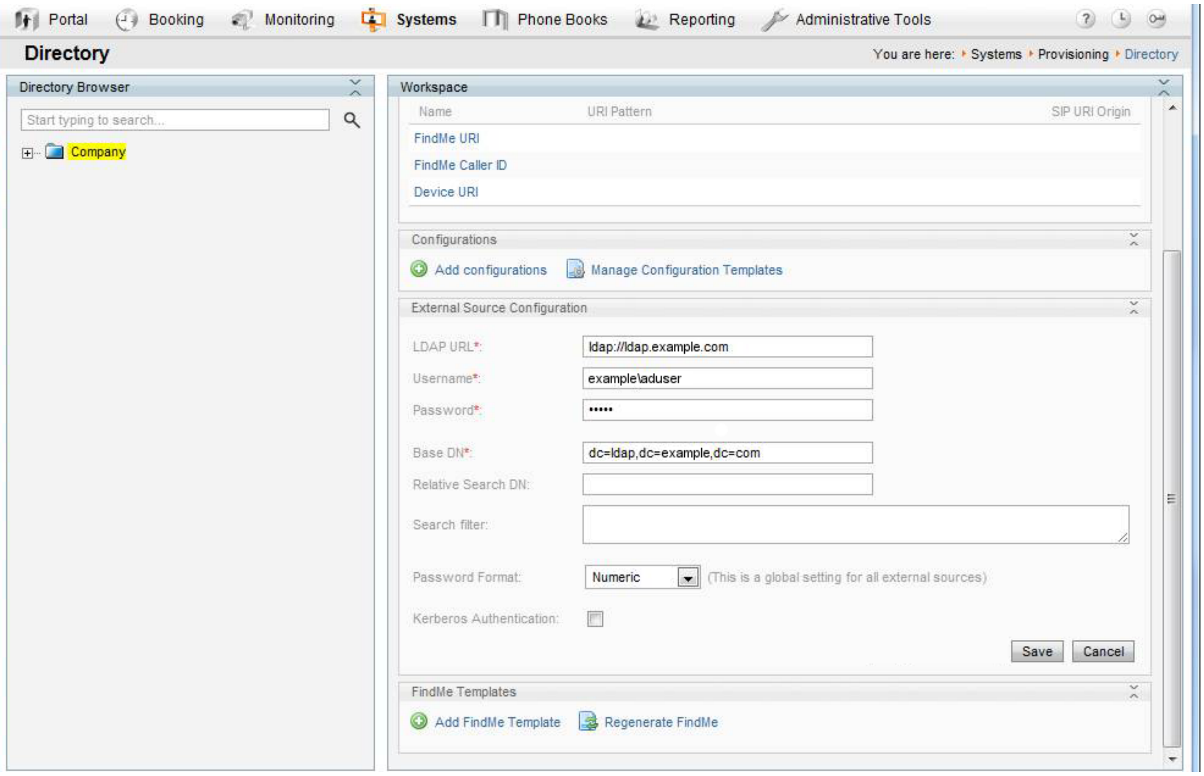
External Source Configuration

Synchronize folder with Active Directory

FindMe Templates

Add FindMe Template   Regenerate FindMe

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



Name	URI Pattern	SIP URI Origin
FindMe URI		
FindMe Caller ID		
Device URI		

Configurations

Add configurations   Manage Configuration Templates

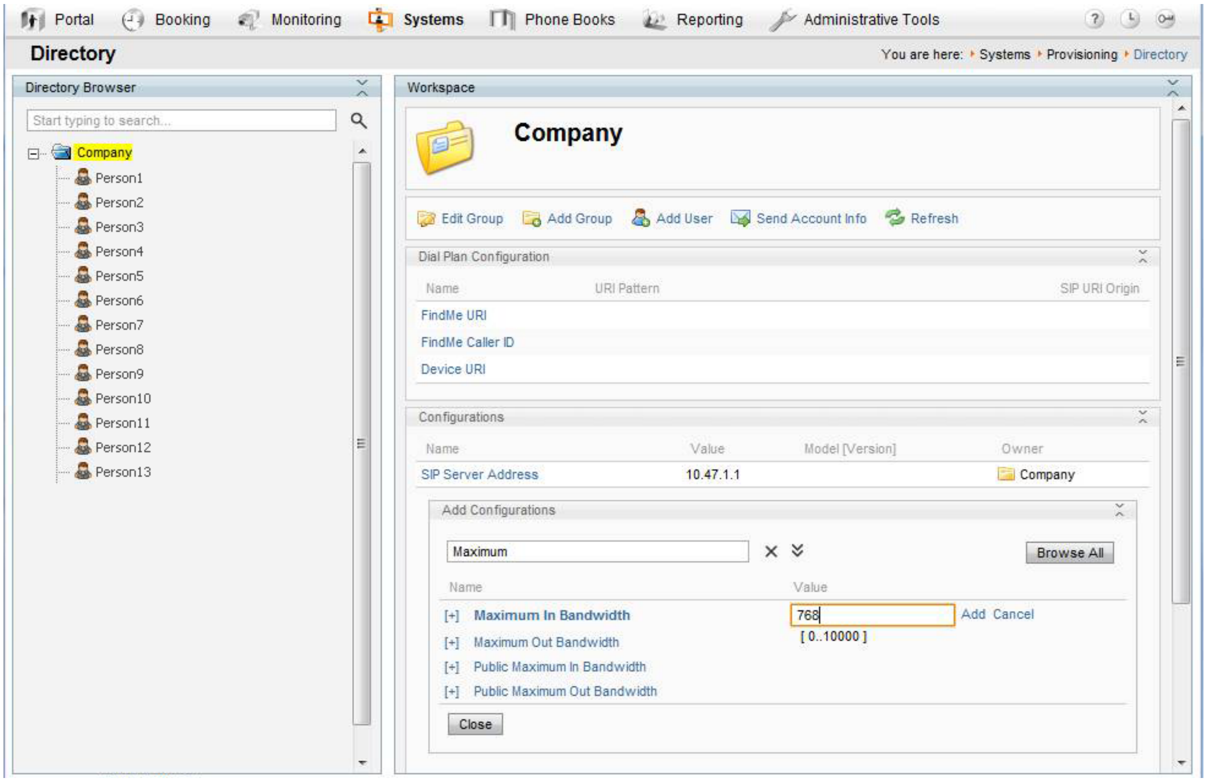
External Source Configuration

LDAP URL*:	ldap://ldap.example.com
Username*:	example\aduser
Password*:	•••••
Base DN*:	dc=ldap,dc=example,dc=com
Relative Search DN:	
Search filter:	
Password Format:	Numeric (This is a global setting for all external sources)
Kerberos Authentication:	□

FindMe Templates

Add FindMe Template   Regenerate FindMe

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



Dial Plan Configuration

Name	URI Pattern	SIP URI Origin
FindMe URI		
FindMe Caller ID		
Device URI		

Configurations

Name	Value	Model [Version]	Owner
SIP Server Address	10.47.1.1		Company

Add Configurations

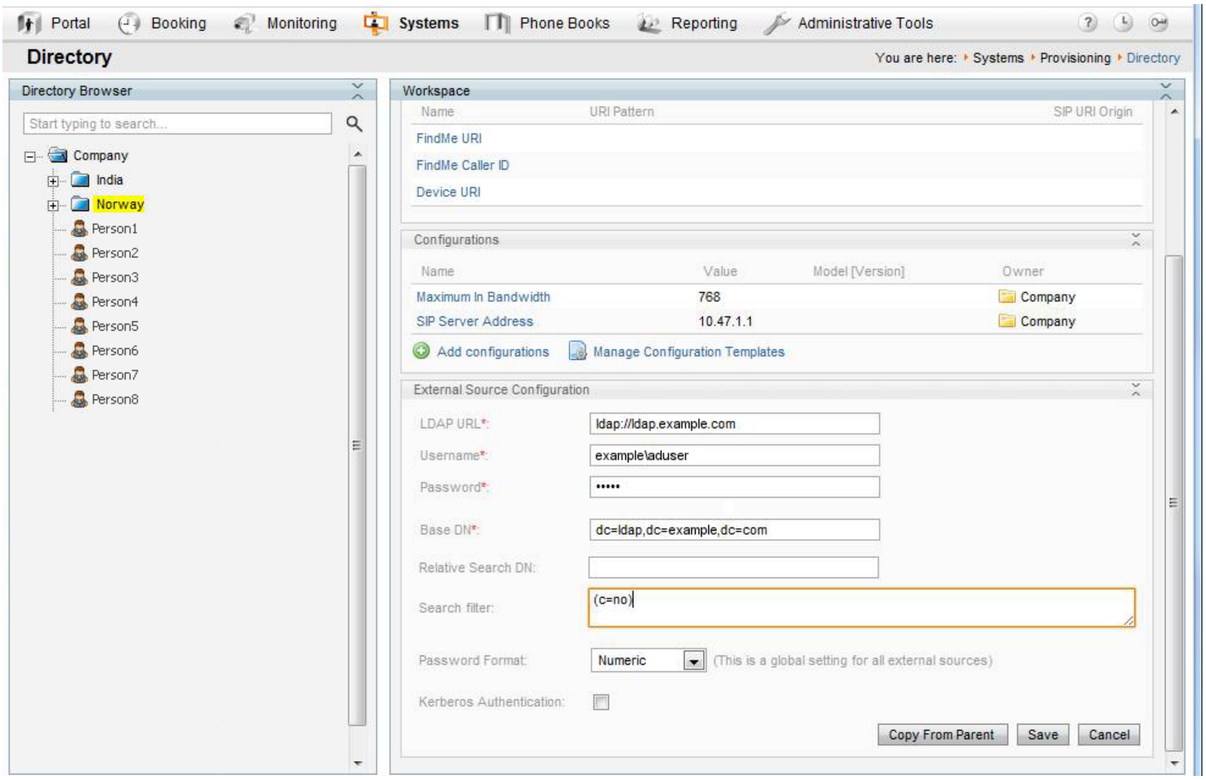
Maximum

Name	Value
[+] Maximum In Bandwidth	768 [0..10000]
[+] Maximum Out Bandwidth	
[+] Public Maximum In Bandwidth	
[+] Public Maximum Out 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.



Name	URI Pattern	SIP URI Origin
FindMe URI		
FindMe Caller ID		
Device URI		

Configurations

Name	Value	Model [Version]	Owner
Maximum In Bandwidth	768		Company
SIP Server Address	10.47.1.1		Company

Add configurations Manage Configuration Templates

External Source Configuration

LDAP URL*: ldap://ldap.example.com

Username*: example\aduser

Password*: •••••

Base DN*: dc=ldap,dc=example,dc=com

Relative Search DN:

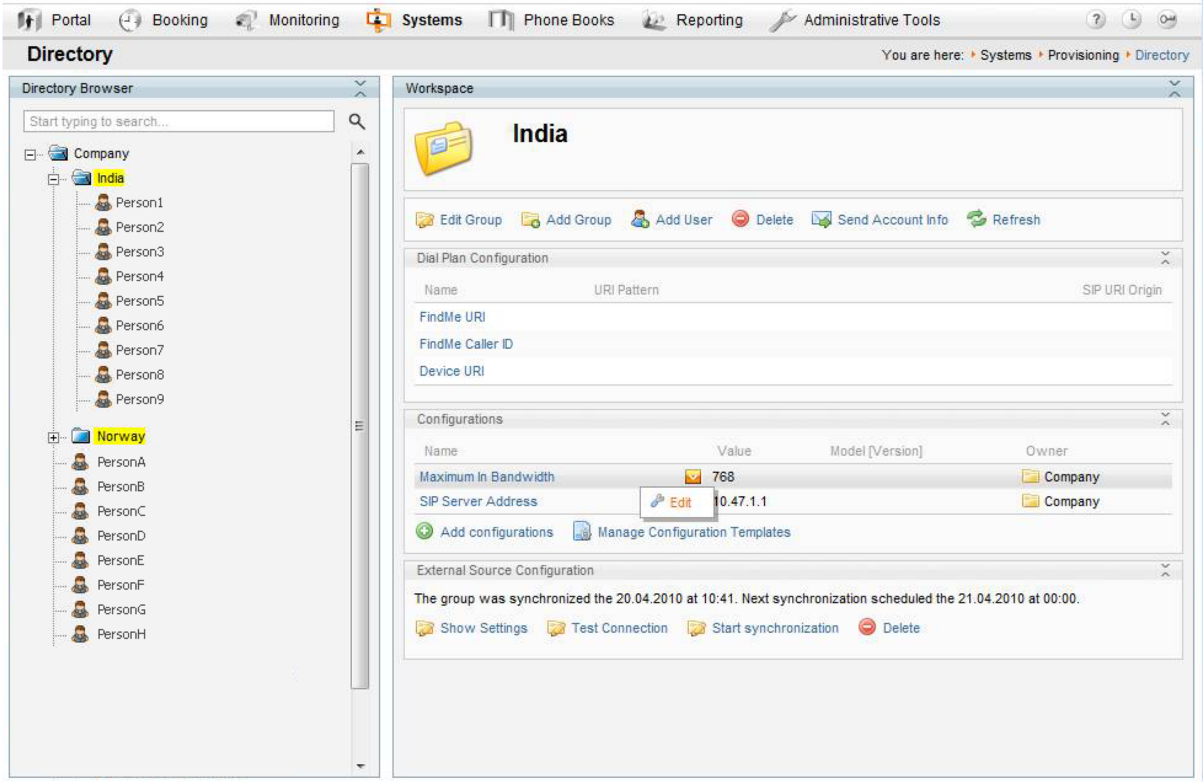
Search filter: (c=no)

Password Format: Numeric (This is a global setting for all external sources)

Kerberos Authentication: □

Copy From Parent Save Cancel

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.



Dial Plan Configuration

Name	URI Pattern	SIP URI Origin
FindMe URI		
FindMe Caller ID		
Device URI		

Configurations

Name	Value	Model [Version]	Owner
Maximum In Bandwidth	768		Company
SIP Server Address	10.47.1.1		Company

Add configurations Manage Configuration Templates

External Source Configuration

The group was synchronized the 20.04.2010 at 10:41. Next synchronization scheduled the 21.04.2010 at 00:00.

Show Settings Test Connection Start synchronization Delete

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*))`**

Configuring a dial plan

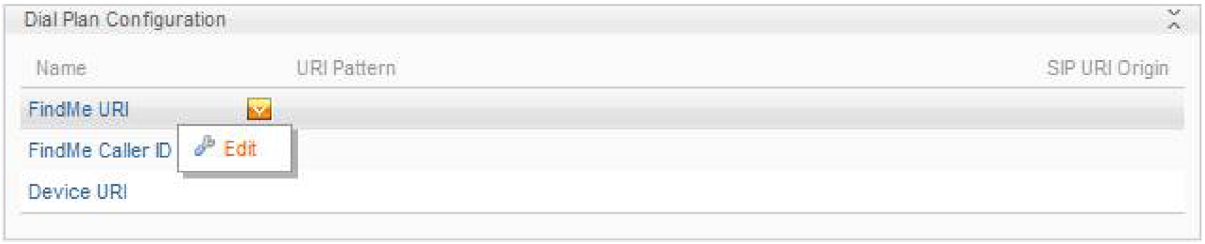
You can use the following user information fields to generate the URI pattern for **FindMe URI** and **FindMe Caller ID**:

- 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)

1. Hover over the **FindMe URI** field and click **Edit**.



2. Edit the pattern appropriately:
   - We recommend using the **`{emailAddress}`** placeholder, where the mail domain must be identical to the SIP domain.
   - Alternatively, use **`{username}`**`@`**`<domain>`**, where **`<domain>`** is the SIP domain configured on your Cisco VCS at **VCS configuration > protocols > SIP > Domains**. Note that the `@` sign must *not* be included in the username.
3. Click **Save**.
4. Repeat the above steps to configure the **FindMe Caller ID** field. The Caller ID is the phone number that will be displayed to the call recipient as callback number if FindMe routes a telepresence call through an ISDN gateway.
5. Hover over the **Device URI** field and click **Edit**.

6. Edit the pattern appropriately:
   - We recommend using the default Device URI Pattern **`{username}.{device.model}@example.com`** to easily identify the type of device the user provisions to (that is, ‘movi' or 'e20') and to maintain unique Device URI Patterns. If more than one user has 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.
   - Include **`device.connectivity`** in the pattern to add the word *internal* for Cisco VCS Control-registered users or *external* for Cisco VCS Express-way registered users to each device URI. A sample Expressway-registered device URI would look like this: **`firstname.lastname.external@example.com`**.
   - In addition you can change the words *internal* and *external* to for example *home* and *office*. The device URI will then be: firstname.lastname.office@example.com or firstname.lastname.home@example.com.
   - Note that you cannot replace "internal" or "external" with a blank/space.

Using Regex

Regex is supported in all **Dial Plan Configuration** fields.

Examples

To remove spaces:

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

To remove spaces and +47:

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

To extract the domain part of the email address:

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

To replace ø with o:

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

Uploading a new configuration template

Each type of endpoint comes with its own XML template file for provisioning. A new template is usually provided with each software release, either included in the software deliverable archive, or downloadable from the same cisco.com page as the product's release notes.

When you have the required templates available locally:

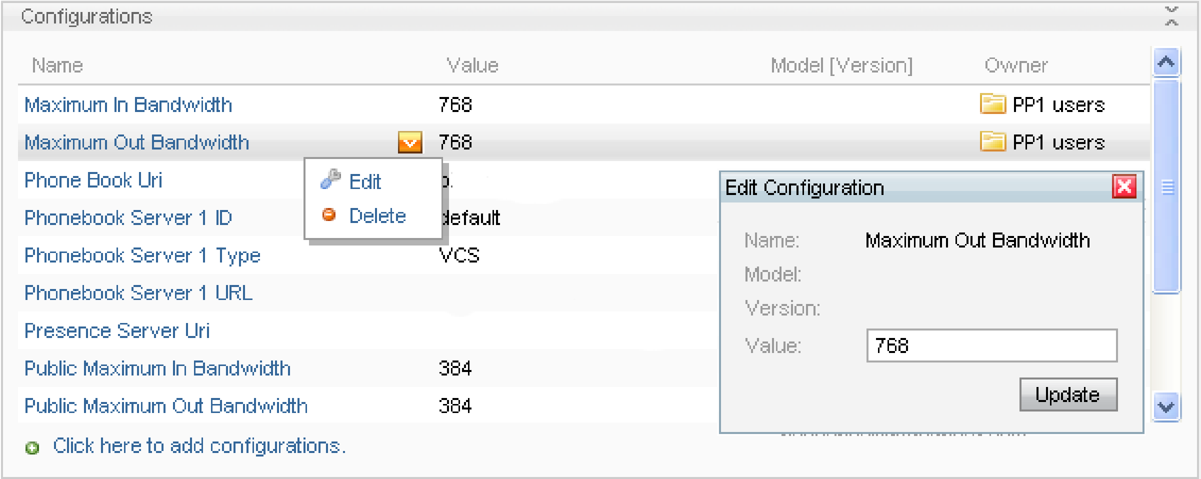
1. Click **Manage Configuration Templates**.
2. Click **Upload New**.
3. Locate and select the configuration template.
4. Click **Open**.

The new template is now available for configuration.

Setting up user configurations

To edit an existing configuration:

1. Hover over the configuration setting name, click the arrow that appears to the right, and click **Edit**.
2. Modify as required. For guidance on the default, available, and recommended settings, see the administrator documentation for each endpoint.
3. Click **Update**.



Name	Value	Model [Version]	Owner
Maximum In Bandwidth	768		PP1 users
Maximum Out Bandwidth	768		PP1 users
Phone Book Uri			
Phonebook Server 1 ID	default		
Phonebook Server 1 Type	VCS		
Phonebook Server 1 URL			
Presence Server Uri			
Public Maximum In Bandwidth	384		
Public Maximum Out Bandwidth	384		

Edit Configuration

Name: Maximum Out Bandwidth

Model:

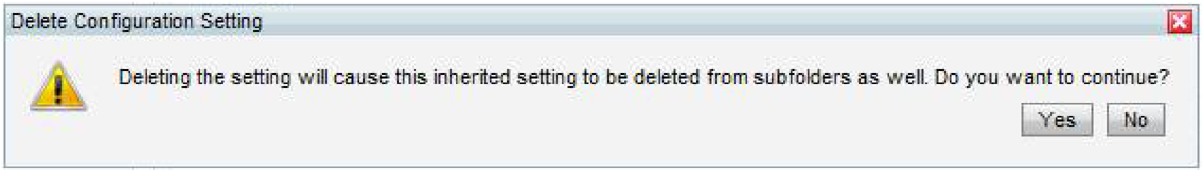
Version:

Value: 768

Deleting 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:



Delete Configuration Setting

Deleting the setting will cause this inherited setting to be deleted from subfolders as well. Do you want to continue?

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.

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	

As a minimum, the sAMAccountName and mail attributes are required to import to the Cisco TMS Provisioning Directory appropriately.

Disabled accounts

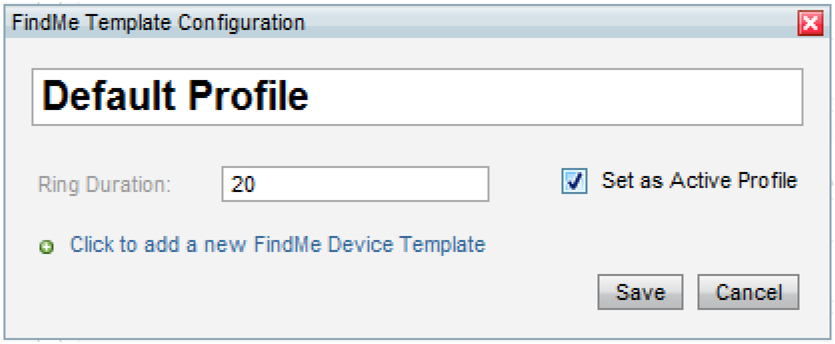
Note that Cisco TMS also filters out anything that is disabled in AD, meaning that if the account is disabled, Cisco TMS does not import it.

If an active account is imported to the Cisco TMS Provisioning Directory and is subsequently disabled in Active Directory, Cisco TMS will remove it from the Provisioning Directory on the next synchronization.

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 from the Cisco TelePresence EX Series and these devices have URIs on the form: `<username>.office@example.com`

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


FindMe Template Configuration

Default Profile

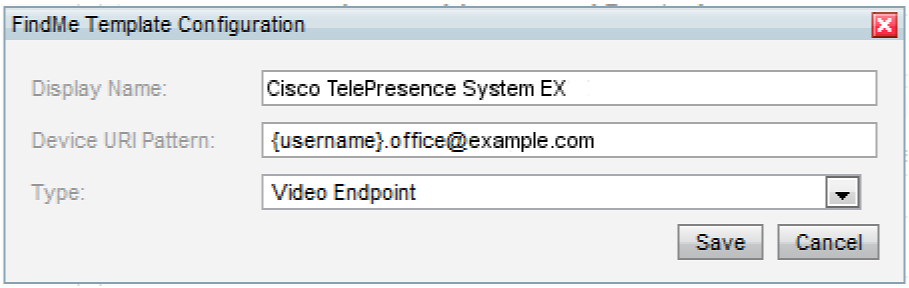
Ring Duration: 20

☑ Set as Active Profile

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

He will have to add a FindMe Device Template to his FindMe Template for the EX series. 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@example.com and the correct type:



FindMe Template Configuration

Display Name: Cisco TelePresence System EX

Device URI Pattern: {username}.office@example.com

Type: Video Endpoint

As Tore has both Jabber Video and E20s in his deployment, he also needs to set up Jabber Video and Cisco E20 endpoints for provisioning. In the **Dial Plan Configuration** pane, he has set the Device URI Pattern to be provisioned with:

`{username}.{device.model}@example.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:

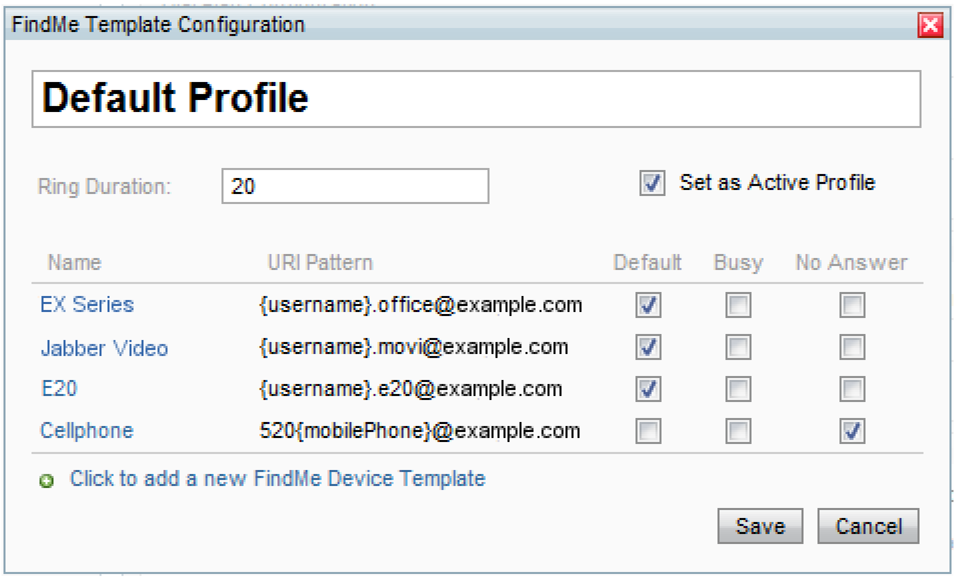
`{username}.movi@example.com{username}.e20@example.com`

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}@example.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:



FindMe Template Configuration

Default Profile

Ring Duration: 20

☑ Set as Active Profile

Name	URI Pattern	Default	Busy	No Answer
EX Series	{username}.office@example.com	☑	□	□
Jabber Video	{username}.movi@example.com	☑	□	□
E20	{username}.e20@example.com	☑	□	□
Cellphone	520{mobilePhone}@example.com	□	□	☑

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.

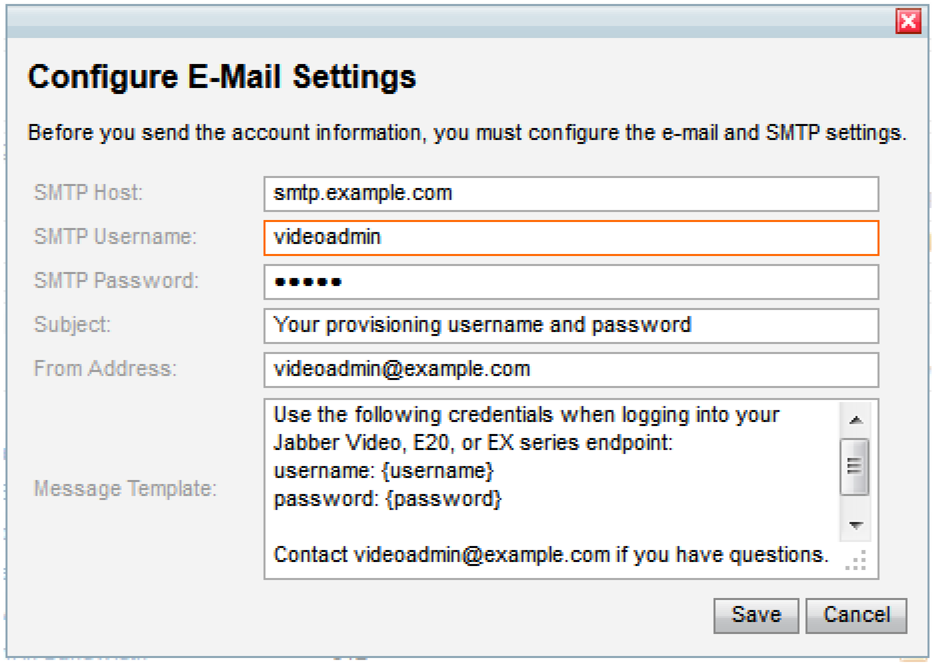
Note: We recommend that whenever changes are made and saved in the FindMe Template Configuration, the Administrator selects **Regenerate FindMe** to ensure all changes are updated appropriately. Selecting **Regenerate FindMe** will replace existing FindMe users' configurations as well as apply configurations 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. A sample template is shown below.
   - The message template must include {username} and {password}, placeholders that will be replaced by each individual's provisioning credentials.
   - If you have configured FindMe for your users, we also recommend including the link to the user FindMe UI on the Cisco VCS in the message.



Configure E-Mail Settings

Before you send the account information, you must configure the e-mail and SMTP settings.

SMTP Host:	smtp.example.com
SMTP Username:	videoadmin
SMTP Password:	●●●●●
Subject:	Your provisioning username and password
From Address:	videoadmin@example.com

Message Template:	Use the following credentials when logging into your Jabber Video, E20, or EX series endpoint:
	username: {username}
	password: {password}
	
	Contact videoadmin@example.com if you have questions.

6. Click **Save**.

Test and send

To test that email settings are working correctly:

1. From the Provisioning Directory browser, select yourself (or another suitable user).
2. Click **Send Account Info**. The **Send Account Information** window will open.
3. Click **Send Email**.
4. Confirm that this email message was received correctly by you or your test user.

You are now ready to send all users their account information:

1. Select the root folder in the Provisioning Directory browser.
2. Click **Send Account Info**. The **Send Account Information** window will open.
3. Click **Send Email**.

Adding a new user

When a new user is included in the Provisioning Directory, either manually or imported from AD, provisioning information will not be sent automatically.

Follow the test instructions above to send the account information to an individual user.

Changing Cisco VCS or cluster

If changing the Cisco VCS or cluster used for provisioning and FindMe, the SIP server address must be update to correspond with the FQDN of the new Cisco VCS or cluster. FindMe profiles must then be regenerated.

If a generic SIP server address is not available in the provisioning directory or folder, Cisco TMS will not be able to regenerate the accounts to the new Cisco VCS or cluster.

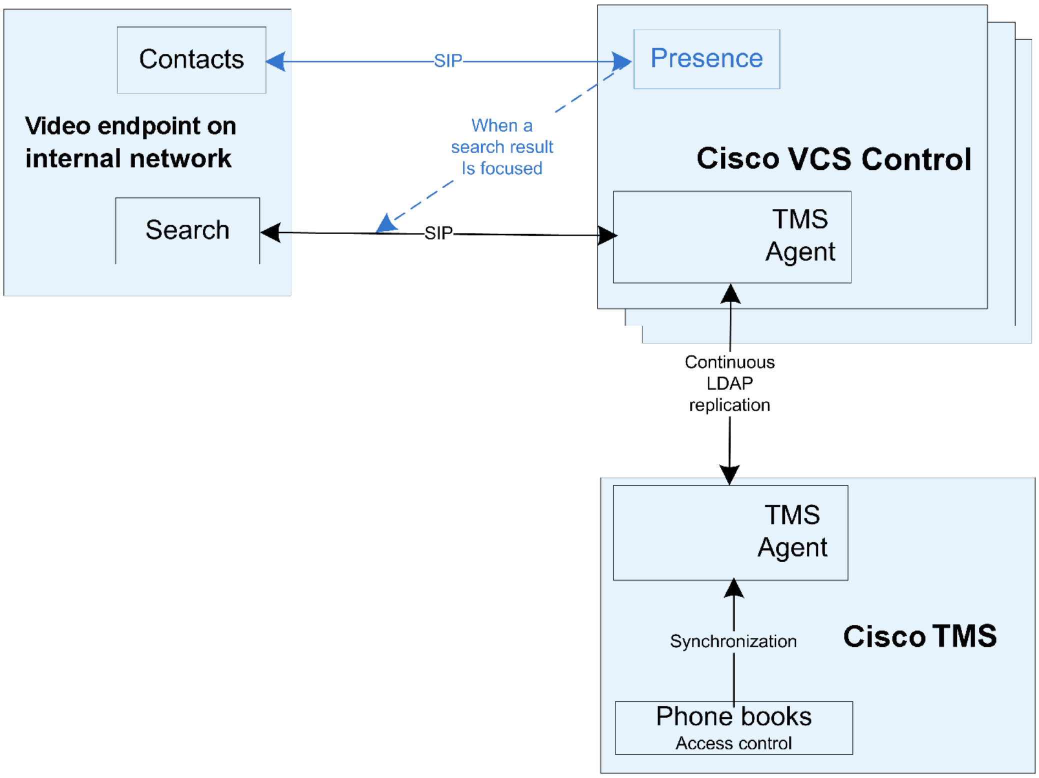
Provisioning phone books

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.

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 Cisco VCS. Users searching with Jabber Video 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 Jabber Video client. Note that blue lines are relevant only to Jabber Video, not to other provisioned endpoints.

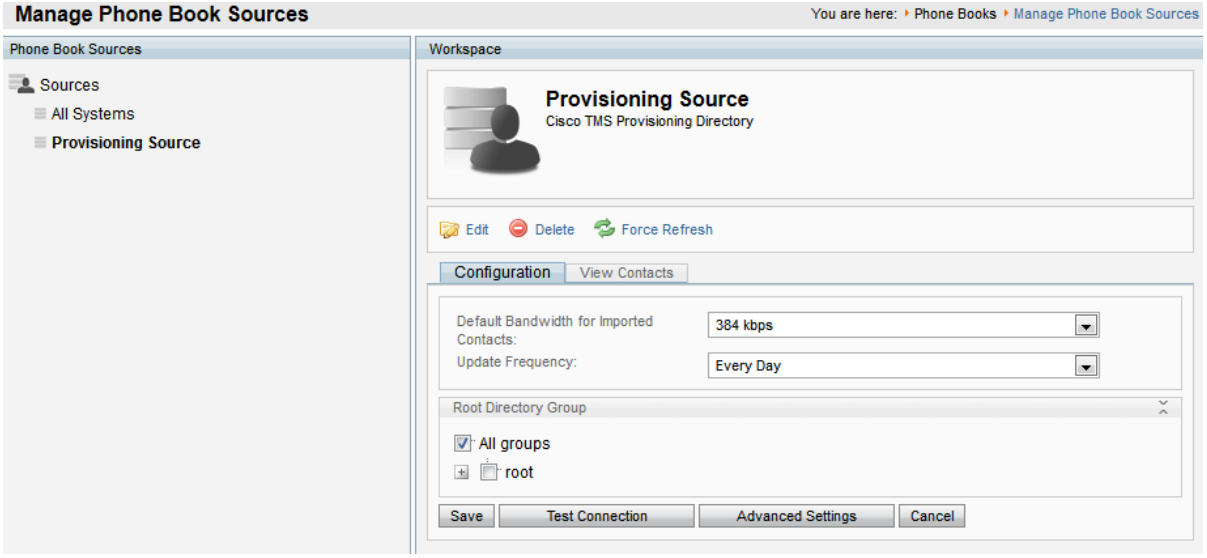


Configuring the provisioning phone book source

Cisco TMS automatically creates a phone book source called Provisioning Source, which includes all users in **Systems > Provisioning > Directory**, and a Provisioning Phone Book based on this source.

If FindMe is not being used, and only the Device URI is being used in the Provisioning Directory, the Provisioning Source will not be populated until devices are provisioned as users begin to log in.

You can see and change the configuration of this phone book source by going to **Phone Books > Manage Phone Book Sources**. In the left-hand pane, click **Provisioning Source**.



Default Bandwidth for Imported Contacts: 384 kbps

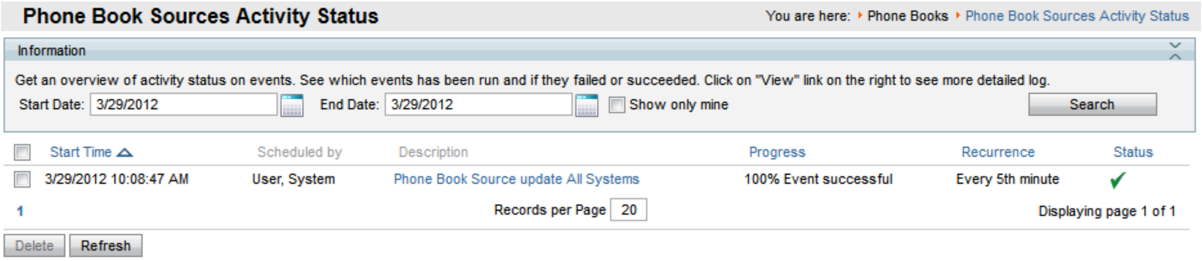
Update Frequency: Every Day

☑ All groups

☐ root

Phone Book Sources Activity Status

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



Phone Book Sources Activity Status
You are here: Phone Books › Phone Book Sources Activity Status
Information
Search
Delete
Refresh

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

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

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

1 Records per Page 20 Displaying page 1 of 1

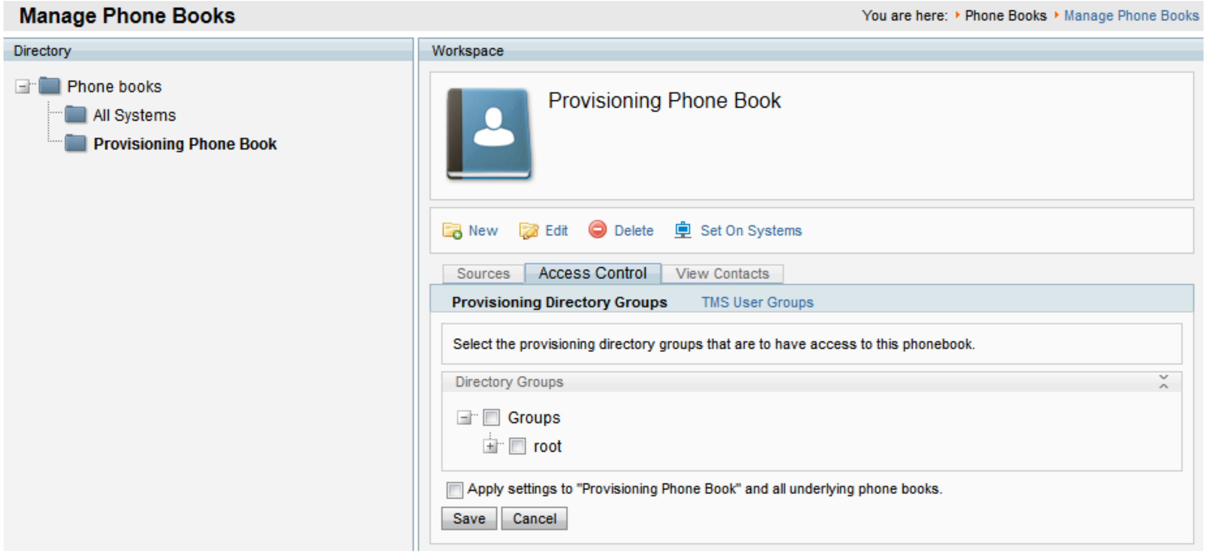
Associating phone book access to groups

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.



Select the provisioning directory groups that are to have access to this phonebook.

☐ Apply settings to "Provisioning Phone Book" and all underlying phone books.

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**.

Setting the provisioning phone book on Cisco TMS-registered endpoints

The provisioning phone books can be set on any Cisco TMS-registered endpoint.

Note that 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 despite the endpoints not supporting SIP. This is due to interworking on the Cisco VCS.

Setting up DNS for Cisco IP Video Phone E20 provisioning

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

In standard Cisco TMS/Cisco VCS 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 TMS/Cisco VCS infrastructure through a Cisco VCS Expressway located outside the company firewall. Consequently, the E20 must be provisioned with an 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/Cisco 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.

Troubleshooting

This section contains:

- Overviews of logs that may be of assistance in troubleshooting provisioning.
- Strategies for resolving provisioning-related problem scenarios in Cisco TMS and provisioned endpoints, with references to error messages that the user or administrator may encounter.

The Cisco TMS Provisioning Directory backend

Diagnostics

In Cisco TMS, you can go to **Administrative Tools > Cisco 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 Cisco VCS(s) to the Cisco TMS and have enabled Cisco TMS Agent data replication on the Cisco VCS or 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 > Cisco 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 **TMS Agent Browser** pane. If a Cisco VCS is in a cluster, expand **Clustered VCSs** from the tree view and then select the 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 Diagnoses** or the **Run All Diagnoses** 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

Diagnostic test	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 Cisco 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

Diagnostic test	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 are 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 **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 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 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 Cisco VCS has one or more subzones configured.	Subzones are set up for the purpose of bandwidth management. An Endpoints/Jabber Video 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 Cisco VCS Administrator Guide.
Verify that Calls to unknown IP addresses is set to "Indirect" on the Cisco 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 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 Cisco 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 > Cisco TMS Agent Settings**.
Verify that the "Device Provisioning" option key is installed on the VCS Control.	See Installing the Device Provisioning option key [p.10] 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 VCS to support publishing of presence status for endpoints that do not support presence.	The configuration must be identical for all Cisco VCSs in a cluster. For more information, see the section on Presence in *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/Jabber Video clients registering to a 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. **CAUTION:** 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 Cisco 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 Cisco VCSs in a cluster. For more information, see section Presence in *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. We recommend 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 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 Cisco TMS 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 VCS in the **System Navigator > Cisco 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 VCS in question. The User Policy option key needs to be installed.	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 > 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 all Cisco 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 VCS **Configuration > Protocols >SIP > Domain**.

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

Reading the Cisco TMS Agent Diagnostics page

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

⛔	Diagnostic shows that your provisioning process has a fatal error.
❓	Diagnostic has not yet been run.
✓	Diagnostic is complete and produced no warnings.
⚠	Diagnostic shows that your provisioning process has an error but it is not critical.
ℹ	Diagnostic shows that there is a non-standard setting in Cisco TMS influencing the provisioning process.
🕒	Diagnostic is pending/waiting/in queue.
⚙	Diagnostic 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.

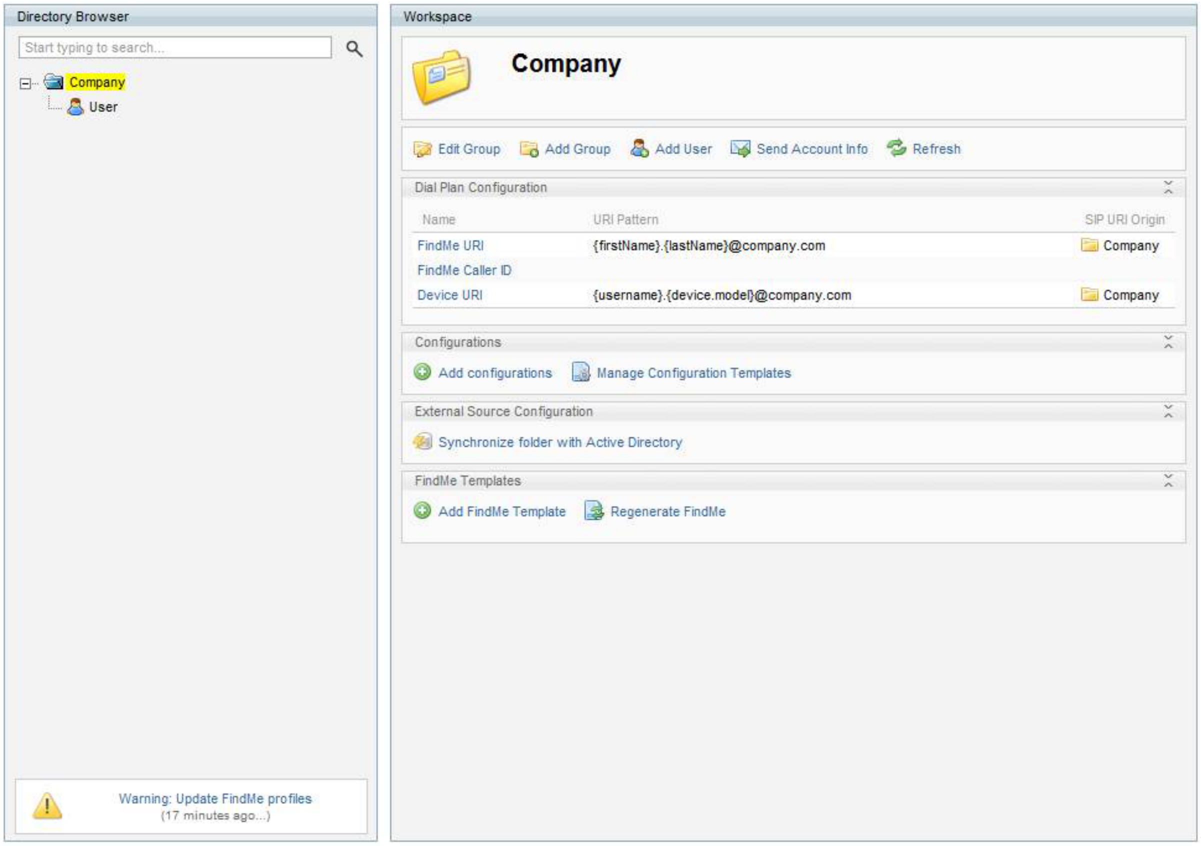
Go to **Administrative Tools > Activity Status** page to see the status of the diagnostics execution. If you enter this page before all tests are completed, you can click **Refresh** to get an up-to-date status.

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.

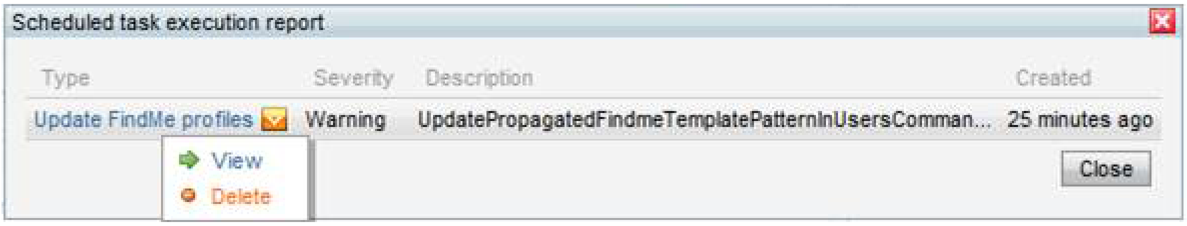


Name	URI Pattern	SIP URI Origin
FindMe URI	{firstName}.{lastName}@company.com	Company
FindMe Caller ID		
Device URI	{username}.{device.model}@company.com	Company

Warning: Update FindMe profiles
(17 minutes ago...)

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.

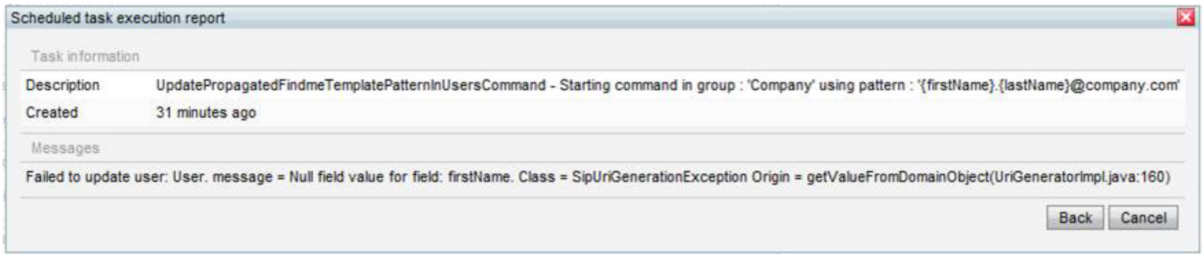
To see a list of scheduled tasks for this warning, click the message in the box.


Scheduled task execution report

Type	Severity	Description	Created
Update FindMe profiles	Warning	UpdatePropagatedFindmeTemplatePatternInUsersComman...	25 minutes ago

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

To delete a message, click the drop-down menu and select **Delete**.



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)

Backend problem scenarios

Provisioning directory not visible in Cisco TMS

If you do not see Directory showing up under **Systems > Provisioning** in Cisco TMS, check the following:

- Are you running Cisco TMS version 13.2? On any Cisco TMS page, check the lower right corner for version information.
- Are you running a trial version of Cisco TMS? Provisioning is not supported in trial versions.
- Do you have have the required privileges to see this directory?
- Has **Enable Cisco TMS Agents (Provisioning)** been set to *Yes* under **Administrative Tools > Configuration > General**?
- On the Cisco TMS server, make sure the TMSProvisioningService is running. Start/restart the service.

Browser error displayed when trying to view Provisioning directory

If, when going to **Systems > Provisioning > Directory**, you receive a browser error page:

- Are you testing directly on the Cisco TMS server, or through a pc/laptop? The former is preferable.
- Do you have the required privileges to see this directory?
- Has **Enable TMS Agents (Provisioning)** been set to *Yes* under **Administrative Tools > Configuration > General**?
- On the Cisco TMS server, make sure the TMSProvisioningService is running. Start/restart the service.
- Directly on the Cisco TMS server, verify that you can browse to the Provisioning Directory by opening the browser and opening the following URL: http://localhost:8787/

Error message after Cisco TMS upgrade: "The Provisioning Directory is not running"

After upgrading Cisco TMS, when navigating to **System > Provisioning > Directory**, whether

- the following error message appears: "The Provisioning Directory is not running or is still initializing. If the TMS Server or TMSAgentService were just restarted, please wait for the Directory to finish initializing. If the Directory does not load after a few minutes, log on to the server and open **Control Panel > Administrative Tools > Services** and restart the TMSAgentService.
- and/or starting the TMSAgentService fails

Follow this procedure:

1. Check the file **log-tmsagentservice.txt** for these lines:
   ```
   10:05:39,297 [4] WARN  TMSAgentWindowsService.TMSAgentWindowsService -
   Service startup...
   10:05:39,313 [4] WARN  TMSAgentWindowsService.TMSAgentWindowsService -
   Starting TMS agent...
   ```

```
10:05:39,545 [4] WARN  TMSAgentWindowsService.TMSAgentWindowsService -
Start script execution failed. Exit Code: 1 Output: Starting Argon
Expecting java located at: D:\Program Files\TANDBERG\TMS\Provisioning\jre
Expecting opends located at: D:\Program
Files\TANDBERG\TMS\Provisioning\OpenDs-2.0
  Error:
```

This confirms that the problem is caused by jar files not being copied into the ... /provisioning/ ... folders on the TMS server.

2. Check the **log-TMSAgent-console.txt** file for a `NoClassDefFoundException`. Details will differ based on which specific jar files are missing.
3. If both criteria above are met, solve the issue by uninstalling Cisco TMS (the application only, leaving the databases untouched) and reinstalling it.

Adding VCS to TMS fails

If you are having problems adding Cisco VCS to Cisco TMS, check the following:

- Is SNMP enabled on VCS? Go to **Administrative Tools > TMS Agent Diagnostics** and run Provisioning Diagnostic Tool test **SNMP** to verify that SNMP is being used on the Cisco VCS.
- Is the SNMP community name being used in Cisco VCS found in list of ‘SNMP Community Names' on the Cisco TMS on page: **Administrative Tools > Configuration > Network Settings**? Note that SNMP community names are case sensitive.
- Is the management address on the Cisco VCS the IP address of the Cisco TMS?
- Use TMS Tools found on the server under **Start > Programs > Cisco** to check and verify SNMP connectivity to the Cisco VCS. In TMS Tools, select **Utilities > Check SNMP**.
- Ensure that SNMP is not being blocked on the network, that is UDP port 161 (both directions).

Error message received when enabling provisioning

If, when creating a new cluster in Cisco TMS and selecting Enable Provisioning, the provisioning fails with the following error message: "Verify that the tmsprovisioningservice is running …", check the following:

- Are you running Cisco TMS version 13.2?
- Are you running Cisco VCS version X7.0 or X7.1?
- Are the time settings in Cisco TMS and Cisco VCS synchronized, preferably using an NTP server?
- Has the Device Provisioning option key been enabled on the Cisco VCS? Go to **Administrative Tools > TMS Agent Diagnostics**, select the Cisco VCS and run **Verify that the "Device Provisioning" option key is installed on Cisco VCS Control.**
- Has the Movi option key been added to Cisco TMS? Go to **Administrative Tools > Configuration > General** to verify this.
- Has **Enable TMS Agents (Provisioning)** been set to *Yes* under **Administrative Tools > Configuration > General**?
- On the TMS server, make sure the TMSProvisioningService is running. Start/restart the service.
- Are there any spaces in the Cisco VCS system names? If so:
  a. Rename the Cisco VCS, removing the spaces.
  b. Restart the Cisco VCS.
  c. Force refresh the system in Cisco TMS for the name change to be updated.
  d. Delete and rebuild the cluster on the Cisco TMS again.

e. Go to **Administrative Tools > TMS Agent Diagnostics** and run **Verifies that all host names in the replication domain can be resolved by doing DNS lookups.**

Importing from Microsoft Active Directory fails

1. Make sure that the URL to the AD Global Catalog server and port are correct, for example **ldap://globalcatalog.company.int:3268?**

   Note: Secure LDAP is not supported.

2. Has the search filter been correctly configured?
3. Make sure the correct username and password are used when logging on and importing from the AD.

Cannot distribute email with username and password

If email distribution of account information to a single user or all users fails, check the following:

- Has the Configure Mail Settings been configured on the **System > Provisioning > Directory > Workspace** pane?

- Is anything on the network blocking SMTP traffic?

Unable to create or edit groups or users in the Provisioning Directory

Corrective actions

- Check the logs for symptoms or error messages. See Provisioning logs [p.50] for more information.
- Restart the TMSAgent Windows service from the Windows Services console.

Provisioning logs

This section describes logs that may be helpful in troubleshooting provisioning. Some of them, like the Jabber Video audit log, are readable to the IT administrator; others will primarily be helpful as debugging tools if you are in contact with customer support.

Cisco TMS provisioning directory logs

If you want to monitor the logs Cisco TMS provides for the provisioning directory specifically, they can be found on the Cisco TMS server at the following location:

```
C:\Program Files\TANDBERG\TMS\wwwTMS\Data\Logs\tmsdebug
```

The names of the relevant log files are:

- **log-TMSAgent.txt**
- **log-tmsagentproxy.txt**
- **log-tmsagentservice.txt**
- **log-TMSAgentDiagnostics.txt**
- **log-TMSAgentReplicationSetup.txt**

If you contact a support representative and need to supply them with logs, you can go to **Administrative Tools > TMS Server Maintenance** and click **Download Log Files** to grab a zipped archive of all logs.

Cisco VCS provisioning logs

In Cisco VCS, go to **Status > Logs > Event Log**.

The Cisco VCS Event Log is displayed on the format date time process_name: message_details. Messages related to the TMS Agent all have the process name tprovisioning.

Use the search field to filter the log by *tprovisioning* so that only TMS Agent messages are showing. For more information on the message_details field of the Status event log, see *Cisco VCS Administrator Guide* for your version.

Jabber Video client logs

There are currently six Jabber Video log files total, as described below.

The Windows application places its log files in **<CSIDL_LOCAL_APPDATA>\Cisco\Logs\**. The **<CSIDL_LOCAL_APPDATA>** folder is typically:

- Windows Vista and Windows 7: **%LOCALAPPDATA% (typically %USERPROFILE%\AppData\Local**
- Windows XP: **%USERPROFILE%\Local Settings\Application Data**

The folder is hidden by default on these systems.

The Mac OS X application places its log files in **~/Library/Logs/Jabber Video/**

Log files created by Jabber Video

File name	Description
Audio.log	Audio-specific information
Audit.log	Communication between Jabber Video and Cisco VCS, see previous section
Client.log	Information related to the client, the GUI and the "business logic" of the client
GStreamer.log	Information from the GStreamer layer
SIP.log	Information from the SIP signalling
TAF.log	Application framework layer information

Log parameters

Logging is controlled by the **Logs.ini** file located in the same folder. This file has one section for each of the log files above. If any parameters are not set for a log file, the corresponding values from the Default section of the file are applied.

The default parameters include:

- The maximum file size is 2000000.
- Two log generations are stored.

Audit.log

The log that will be most useful to you as an administrator is Audit.log. Here, provisioning communication between Jabber Video and the server is recorded. By looking at the audit log you can tell which advanced settings the user has, and whether provisioning succeeds or fails. Some error messages from the server are also recorded here.

Note: The parameters for Audit.log are not in Logs.ini and cannot be edited.

Cisco IP Video Phone E20 logs

E20 includes a web server that can be used to manage the endpoint. You access it by opening its IP address in a web browser (http://<your.IP.address>).

To find your E20's IP:

1. On the E20, go to **Menu > System information**.
2. Under **NETWORK**, you will find the endpoint's **IP address**.

Logs can be viewed and downloaded from the **Logs** tab on the page that opens.

Removing provisioning from a Cisco VCS

If provisioning is no longer required or if provisioning was accidentally enabled on a Cisco 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**.

Bibliography

All documentation for the latest version of Cisco TMS can be found at http://www.cisco.com/en/US/products/ps11338/tsd_products_support_series_home.html

Title	Reference	Link
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
Cisco TelePresence Video Communication Server FindMe Deployment Guide (X6)	D14525	http://cisco.com

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

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

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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

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

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