Cisco TelePresence Management Suite

Installation and Getting Started Guide

Contents

Introduction

Cisco TelePresence Management Suite (Cisco TMS) is a portal for managing and monitoring your videoconferencing network from a single, structured overview. Cisco TMS provides centralized control for on-site and remote video systems, and a deployment and scheduling system for your entire video network.

Cisco TMS automates system configuration for a basic telepresence network, operating right out of the box. You can tune Cisco TMS behavior to suit your organization's needs, set up user permissions, and configure your network model so that all of Cisco TMS call handling functionalities are available.

This document provides information for fresh installations, upgrading an existing version, or configuring the Cisco TMS version that comes preinstalled on a Cisco TelePresence Management Server. Instructions for uninstalling the software are also included.

After installing Cisco TMS, refer to the Getting started with Cisco TMS section of this document for guidance on initial access and setup.

Tip: By clicking the question mark icon (?) on any Cisco TMS page you will access the built-in user guide.

For further information on specific implementation scenarious involving redundancy and secure setups, see the References and related documents section of this document.

Requirements and prerequisites

This section covers hardware and software requirements, and other considerations and dependencies that must be reviewed before installing or upgrading Cisco TelePresence Management Suiteand Cisco TelePresence Management Server:

- Server requirements for installing Cisco TMS. These apply only to customers installing on their own server.
- Provisioning requirements. If using or planning to use the provisioning features of Cisco TMS, refer to this section.
- Client software requirements. These requirements apply to anyone needing to access the Cisco TMS web interface.
- Server network dependencies Dependencies that must be reviewed before installing Cisco TMS or setting up Cisco TelePresence Management Server.
- Ports used by Cisco TMS
- Compatibility with integration products.
- Upgrade notes. Changes to requirements and caveats that upgrading customers should be aware of before starting the upgrade process are listed here.

Server requirements for installing Cisco TMS

The below requirements are specific to installing Cisco TMS on a customer-supplied server.

Hardware requirements

Pentium-compatible processor	2 GHz or higher.
Memory	■ 2 GB RAM or more is recommended. A warning will be displayed during installation if less than 2GB is detected. ■ 4 GB RAM is the recommended minimum for installations on Windows Server 2008 64 bit.
Disk Space	■ 4 GB for installation and application footprint. ■ Additional space is required if you are installing the SQL Server locally–see the Database server requirements section below.

Shared and virtual servers

Cisco TMS is resource intensive with specific server requirements, that increase with the activity level and size of the video network being managed. Using a server hosting other applications or websites for hosting Cisco TMS is therefore not supported.

Cisco TMS can be installed in a virtualized server environment as long as the virtual machine hosting Cisco TMS is allocated sufficient dedicated resources to meet the server and hardware requirements for installation. The resources allocated to the Cisco TMS server instance must be dedicated, and not shared with other server instances. Cisco TMS has been tested in virtual machines using VMWare ESX and Microsoft Virtual Server 2007.

OS and software requirements

Product	Version	Additional notes
Windows Server	- Windows Server 2003 SP1 or later, 32 bit - Windows Server 2003 R2 SP1 or later, 32 bit - Windows Server 2008 Standard 32 bit and 64 bit - Windows Server 2008 R2 Standard 64 bit	- The server operating system must be English, Japanese or Chinese. - Standard/Enterprise/DataCenter editions all supported on both Windows Server 2003 and R2. - Using the latest service pack is recommended for all versions.
.NET Framework	4.0	- Must be installed prior to running the Cisco TMS installer. - Cisco TelePresence Management Suite Analytics Extension (Cisco TMSAE) requires .NET 3.5.
Windows SNMP Services		Checked for and usually installed automatically if not present. Depending on your type of installation, the Windows installation CD may be required.
IIS	- For Windows 2003: IIS 6 - For Windows 2008: IIS 7	Will be installed automatically by the Cisco TMS installer unless already present on the system.
Windows Installer	4.5	If not present on the system, the Cisco TMS installer will inform you that the installation is needed before continuing, and the installation package is provided for you.

Access requirements

- Administrator access to the Windows server and database; if an existing database server is to be used, you must have the login information to be used as the Cisco TMS service account (see Database server requirements).
- For the proper installation of the OpenDS and Provisioning components, MS DOS or access to execute *.cmd and *.bat files (not necessarily the command prompt) must be available on the server during installation and upgrades.

Database server requirements

Cisco TMS stores all its customer data in its SQL database named tmsng. This self-contained storage allows for convenient backup and recovery of customer information. For new installations, the installer creates tmsng using the SQL server defaults. Upgrades will reuse an existing Cisco TMS database.

Disk space

Required database disk space depends on the size, auditing, and activity level of the video network. In order to control the growth of the database, purge plans for logs and events can be set in the **Administrative Tools > Cisco TMS Server Maintenance** page. Most installations require 1-4 GB for database growth. To see the options available for ongoing Cisco TMS database information and maintenance tasks, go to the **Administrative Tools** menu.

SQL server version

One of the following is required:

Product	Version	Additional notes
Microsoft SQL Server 2008	All versions, 32 bit or 64 bit	If there is not an SQL database present on the server when installing Cisco TMS, Microsoft SQL Server 2008 Express 32 bit will be installed.
Microsoft SQL Server 2005	All 32-bit versions	Express Edition has a 4 GB database size limit, large deployments with databases that can be expected to grow larger than 4 GB must use the full edition.

Local versus remote server

During installation, you can chose between using an existing SQL Server or having Cisco TMS install SQL Server 2008 Express locally on the Cisco TMS server. The compatibility level will be set automatically by the installer; 100 for SQL Server 2008 and 90 for SQL Server 2005.

The database server that Cisco TMS is connected to may be installed on the same server as Cisco TMS or on a separate SQL server, and this is an option at installation.

Running SQL on a separate server is strongly recommended for large (100+ system) or high-usage video networks because there are performance benefits due to the high memory and disk I/O load associated with running an SQL Server. Hosting the database server separately from the Cisco TMS server frees up memory and disk resources, improving Cisco TMS's performance. Note that if the database is on a separate server, the database name must still be **tmsng**.

Database permission requirements

Mixed Mode Authentication must be enabled on the database server. Windows Authentication is not supported.

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

- Automatic setup, but with security limited role. Ask your SQL server administrator to create an SQL user and login that has the *dbcreator* and *securityadmin* server roles. This account will be the service account for Cisco TMS. When prompted for SQL Server credentials during installation, enter the username and password for that account. Cisco TMS will create the tmsng database automatically

using the server defaults, assign itself as the owner and continue to use the supplied account to access the database after installation.

- Manual database creation, max security limited role. Ask your SQL server administrator to create:
  - A database named tmsng with the appropriate options. The database collation must be Latin1_General_CI_AIS.
  - An SQL user and login to use for the Cisco TMS Service account and grant the user the *dbowner* role for the tmsng database.

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

Performing SQL database backups

Follow best practices and take regular backups of the database to ensure that you can recover and restore the system in case of a system failure or as part of a larger disaster recovery plan.

Additional help on performing SQL backups is available in the *Cisco TMS Database Knowledge Tips* document. Backups should be stored away from the Cisco TMS server for maximum protection.

TMS Agent database backup

To perform a backup of the TMS Agent database, go to **Administrative Tools > Configuration > TMS Agent Settings**. The installer automatically places the provisioning database (OpenDS) backup in the Cisco TMS backup folder (by default, **<TMS folder>\wwwTMS\Data\Backup\opends**).

Provisioning requirements

If using the provisioning directory features of Cisco TMS 13.1, Cisco VCS version X5.2 or later is required.

Cisco TelePresence Management Server only: We recommend the Provisioning Directory be limited to a maximum of 5000 users.

Client software requirements

Both administrators and users access Cisco TMS via a web interface. A Windows username and password to the Cisco TMS server is required; either a local machine account, or a domain account if the server is joined to a domain.

The following are the software requirements to access Cisco TMS:

Web browser	One of the following: ■ Microsoft Internet Explorer 7.0 or later ■ Firefox 3.6 or later
Java Runtime Environment (JRE)	■ Version 1.5 required ■ Version 1.6.0 or later recommended JRE is required for using the **Monitoring** pages in Cisco TMS. If it is not installed, most browsers will prompt you to download and install the browser plug-in automatically. If this is not possible due to security restrictions, install it manually on the client computer from the JRE installation file which can be downloaded from http://www.java.com.

Server network dependencies

The following network dependencies must be considered:

- Domain membership preferred: Each user logging into Cisco TMS needs a Windows User Login to authenticate to the web site. Users must have either a local account on the Cisco TMS Windows Server or a Domain account that the server trusts through Active Directory. By making the server a member of the domain, all trusted domain users can automatically use their existing Windows credentials to log into Cisco TMS. (You can still limit what users can do after they have logged into Cisco TMS using Cisco TMS permissions. Active Directory membership is the recommended deployment for most installations because it avoids creating local Windows accounts for each user.)
- Cisco TMS website accessible by IP and Hostname: not all devices support DNS hostnames or Port Numbers, the Cisco TMS web site must therefore be accessible by an IP Address on port 80. Some functionality requires Cisco TMS to be reachable by hostname; therefore Cisco TMS should also be accessible by a fully qualified hostname.
- Mail server access: Cisco TMS requires access to an SMTP server to be able to send email. Your company's existing mail servers can be used for this. Note that Cisco TMS supports SMTP Auth login for authentication if required.
- Network access to managed devices:Cisco TMS needs specific protocols and access to manage devices. Any network firewalls or NAT routers must allow traffic to flow to and from Cisco TMS.
- For installations using the Cisco TMS Provisioning Directory for Cisco Movi and Cisco IP Video Phone E20, or Cisco TelePresence System EX series deployments, 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 installation or upgrade, ensure that the DNS servers used by Cisco TMS contain forward lookups for the Cisco TMS server. DNS reverse lookups (PTR records) that were required in Cisco TMS 12.5, are no longer required.
- If installing Cisco TMS on a customer-supplied server, IIS components ASP.NET and ASP must be enabled.
- Windows Server 2008 only: the Windows Firewall feature is enabled by default and controls both inbound and outbound ports. Refer to the Ports section for information on which ports must be opened if Windows Firewall is enabled.
- Make sure anti-virus programs or other security measures are not blocking applications from sending mail directly using the SMTP port (TCP Port 25).

Ports used by Cisco TMS

The following ports are used by Cisco TMS and must be enabled in the Windows firewall. Not all services will be used in all installations depending on the configuration and the devices used.

Service	Protocol	Port	Direction (relative to Cisco TMS)	
			In	Out
HTTP	TCP	80	X	X
HTTPS	TCP	443	X	X
Telnet	TCP	23		X
Telnet Challenge	TCP	57;		X
Telnet Polycom	TCP	24	X	X
FTP	TCP	20, 21		X
SNMP	UDP	161	X	X
SNMP Traps	UDP	162	X	X
SMTP	TCP	25		X
LDAP	TCP	389	X	X
LDAPS	TCP	636	X	X
TMS-Agent	TCP	8989	X	X
Polycom GAB	TCP	3601	X	X
Polycom MGC (for version 6 and lower)	TCP	5001	X	X
TMS Agent Admin	TCP	4444	X	X

Note: Cisco TMS cannot use multiple network cards on a server: and will only bind to the first available network interface. Cisco TMS can manage a public and private network so long as the public network's connection is further upstream from Cisco TMS, rather than being directly connected to Cisco TMS (using multiple network interface cards).

Compatibility with integration products

Compatibility with integration products does not change for this release.

Note: The most recent version is required for all features and fixes to be available.

Product	Version
TANDBERG See&Share	3.3
Cisco TelePresenceManagement Suite Extension for Microsoft Exchange	All versions
Cisco TelePresenceManagement Suite Network Integration Extension	All versions
Cisco TelePresence Management Suite Extension for IBM Lotus Notes	All versions
Cisco TelePresenceManagement Suite Extension Booking API	All versions

Upgrade notes

Upgrading Cisco TMS software is handled automatically by the installer, and there is no need to uninstall previous versions prior to upgrading.

Review all notes listed below that apply to the version of Cisco TMS you are currently running before starting your Cisco TMS upgrade.

All upgrades

The default Booking Confirm email templates and phrase files have been updated in 13.1. If you have customized these templates, the new additions are not automatically added to your customized files but are still available for use. To see the default usage of these new values and have them in your templates, customers with customized Booking Confirm templates or phrases must use the **Revert to Default** button in the **Edit Email Template** page. Once defaulted, you can re-add the customizations back into the templates or phrase files.

Version-specific notes

Versions prior to 13.0

If upgrading from a version prior to 13.0, note that:

- .NET Framework requirements have changed from 3.5 to 4.0.
- The Cisco VCS requirement for provisioning has changed to version X5.2 or later.

Version 12.5 and older

DNS reverse lookups (PTR records) that were required in Cisco TMS 12.5, are no longer required. Note that the same requirement applies to the Cisco VCS. See the *Cisco VCS Software Release Notes (X5)*.

Under **Administrative Tools > General Settings**, **Enable TMS Agents** is now set to *No* by default. If enabling this setting, we recommend going to **Administrator Tools > TMS Agent Diagnostics** to confirm that the local TMS Agent shows no errors and that all diagnostic tests are OK.

If any errors are found on the Local Cisco TMS Agent, these errors need to be fixed before proceeding with replication to the Cisco VCS(s). Refer to the Diagnostic section within the *Provisioning Deployment Guide* for troubleshooting any errors found on the Local Cisco TMS Agent or contact your local Cisco partner or customer support for assistance.

Versions 12.2 and 12.1

If your installation uses the Cisco TMS Provisioning directory functionality for Cisco Movi deployments and you are upgrading Cisco TMS from either software version 12.1 or 12.2, you must follow the upgrade procedures in the document Cisco VCS Deployment Guide – Cluster creation and maintenance (VCS X5).

Caution: Upgrades will be blocked if the procedures found in the deployment guide are not followed appropriately. The error message will state that Provisioning on all clusters must be disabled before upgrading.

Versions prior to 12.2

If you are upgrading from a version older than Cisco TMS 12.2, the onetime database clean-up included in the Cisco TMS 12.2 release will be executed during installation. For most installations, this step only adds an additional minute or two, but for a large installation it can take 30 to 60 minutes depending on the performance of the SQL server, the type and number of calls scheduled in Cisco TMS, and the participant counts.

This step is performed automatically and you see an"Upgrading" notification. The process bar may not move but the installation is still running. *Be patient.* Do not stop or attempt to stop the installation process during this step.

For detail about this update, refer to the release notes for Cisco TMS 12.

Version 12.0

Customers who had Cisco VCS clusters defined in Cisco TMS 12.0 should review the clustering section of the Provisioning Deployment Guide for instructions on changes to cluster configuration with VCS X4.1 software.

Customers who plan on using the Provisioning Directory should review the *Cisco TelePresence Provisioning Deployment Guide* to understand the software dependencies between Cisco TMS and VCS.

Versions 11.x and older

The server requirements for Cisco TMS have changed since these Cisco TMS versions, including removing support for Windows 2000 Server and Microsoft SQL Server 2000.

Upgrading or migrating servers

- If you are using an older version of SQL Server, you must upgrade the SQL software *before* upgrading or installing Cisco TMS.
- Customers wanting to move the Cisco TMS database to a new server should move the database and/or database server prior to running the installer. Use the standard Microsoft SQL tools (the Cisco TMS database is named 'tmsng'), and then select *Custom* during the installation to specify the database location.
- If you are upgrading from Windows Server 2000 to Windows Server 2003, Microsoft recommends performing a clean installation.
- We recommend backing up the Cisco TMS database, along with any customized customer files, before upgrading Windows. After the Windows upgrade, reinstall your original Cisco TMS version and restore the database backup. Then upgrade to the latest version of Cisco TMS. Additional assistance on backing up and restoring Cisco TMS can be found in *Cisco TMS Database Knowledge Tips*.

Recording Servers requirement change

If you are using Cisco TelePresence Recording Servers with Cisco TMS, the Recording Servers must be running software greater than S2.0. If you are upgrading from versions prior to S2, update the configuration between the servers and update any future bookings see the Supplement Notes for Manuals section of the Cisco TMS 11.6 release in document D50418 Cisco TMS v11 Release Notes available from our website.

Permission changes

Starting with Cisco TMS 12.0, the permissions were slightly reorganized compared with previous versions. Administrators who implement different user levels through permissions should review their user group permissions after upgrading to Cisco TMS 12 and adjust the permissions to their intended settings.

Versions 10.x and 9.x

Cisco TMS has gone through significant changes since these releases, and while the Cisco TMS installer will import existing data, there are many new settings and existing settings that have changed.

Work through the **Administrative Tools** settings after installation to populate and update the Cisco TMS configuration to your environment's needs. In particular, the permissions model has been overhauled and Group Permissions and System Permissions must be reviewed and updated to match your needs. Expect inconsistent behavior between different systems until Cisco TMS has refreshed the configuration of each system – normally this will happen automatically within 1-4 hours.

Versions prior to 9.x

For installations older than Cisco TMS 9.0, the Cisco TMS installer will import your existing data, but we recommend performing a new installation rather than an upgrade. Server requirements, configuration, and functionality have changed significantly since these versions.

Installing or upgrading Cisco TMS

Before you start the installation make sure that you have:

- software downloaded from Cisco.com
- release and option keys ready
- considered all relevant Requirements and prerequisites for an installation in your environment

If you are upgrading rather than installing for the first time, also perform any necessary operations described in the section Upgrade notes.

The installation/upgrade process has two parts. After completing an initial setup process, the next process will depend on whether you choose a complete or custom installation.

Note: You may be prompted to reboot the server more than once during installation. The installer automatically resumes after the server reboots.

The installation process has two parts, where the second part is different depending on whether you choose a "complete" or "custom" installation.

Initial installation

Note that depending on Windows components needing to be added, you may be prompted to reboot the server more than once during installation. The installer automatically resumes after the server reboots.

1. Close all open applications and disable virus-scanning software.
2. Extract the Cisco TMS .zip archive to a folder.
3. Run the Cisco TMS executable.
4. Select the language to use for the installer and click **Next**. Note that this language choice does not affect Cisco TMS after the installation.
5. The installer now checks whether the server has the required software components already installed. A warning or error message may be displayed depending on your server's configuration. Follow the prompts and install any missing components.
6. If an earlier version of Cisco TMS is currently installed, you are prompted to upgrade.
   - Click **Yes** to continue. Upgrading removes the old version and upgrades the existing Cisco TMS database.
   - Click **No** to abort the installation and leave the current installation untouched.
7. A welcome window is displayed. Click **Next** to continue.
8. Click **Yes** to accept the license agreement.
9. Select *Complete* or *Custom* and click **Next**.
   - *Complete* uses the default settings. It can be used for upgrades of existing installations with both local and remote SQL installations, and is the recommended choice for performing upgrades. Proceed to the section "Complete" installation below.
   - *Custom* allows you to specify all the options such as the installation path and SQL server choices. Proceed to the section "Custom" installation below.

"Complete" installation

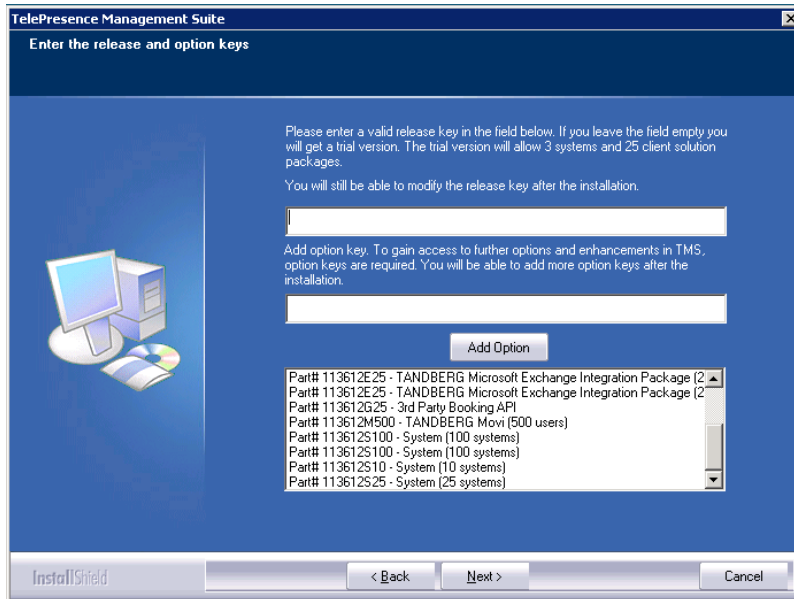Follow the steps in this section if you selected the *Complete* installation option.

Installing or upgrading the database

The installer now searches for an existing SQL Server and Cisco TMS database:

- If an existing database connection is found, the specified SQL Server is used. When prompted, enter the username and password to connect to that SQL server and click **Next**.
  - Click **Yes** to upgrade the existing database to the current version and retain the existing information.We recommend that you back up the database before it is upgraded.
    - The backup is optional. To skip it, click **Next**.
    - To perform the backup:
      i. Enter a path for the backup file and filename, or click **Browse** to navigate to a folder. The backup is done on the SQL Server itself, so these values are local to the SQL Server.
      ii. Click **Backup** to start the backup.
      iii. When the backup is complete (this may take several minutes), click **Next**.
  - Click **No** to stop the installer and manually remove the database from the SQL server if you wish to use that SQL Server and install a new Cisco TMS database.
- If no existing Cisco TMS database connection is found, the installer looks for an SQL installation on the local server.
  - If one is found, enter a user name and password to connect to that server so that the installer can create a new Cisco TMS database.
  - If no local SQL server is found, a local copy of SQL Server 2008 Express Edition is installed and a new Cisco TMS database is created.:
    i. When prompted, enter a password to set for the sa account (administrator) for the new SQL Server installation. Note that if the Cisco TMS server is in a domain or you have a local policy that has a strong password policy, you must use a strong password for the SQL installation.
    ii. Be sure to make a note of the sa password somewhere secure because it is required for future upgrades and Cisco TMS maintenance.
    iii. Click **Next** to proceed with the installation.

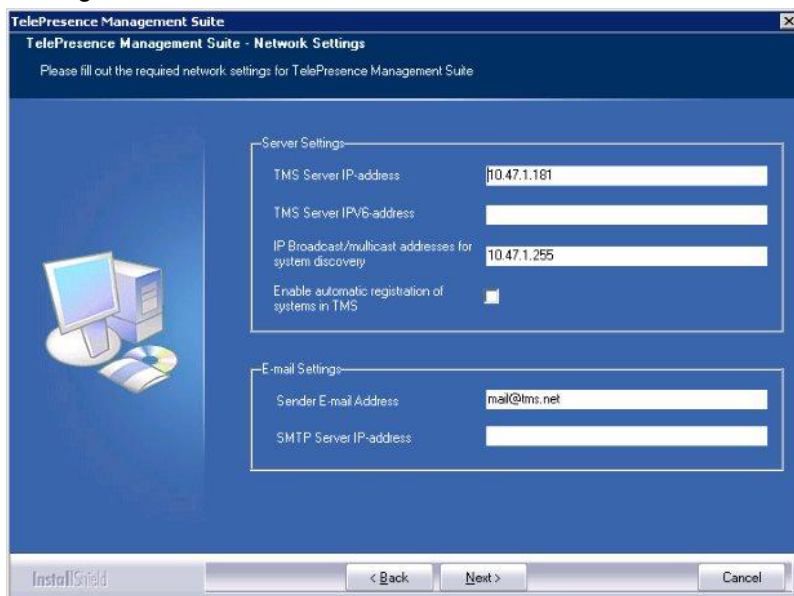## Activating and pre-configuring the installation

1. The **Release and option keys** dialog is now displayed and any existing keys are shown if upgrading. Enter the key(s) to enable additional systems, extensions, or features. A new release key is also required when upgrading to a new major release. The release key must be entered before adding option keys, which are validated as they are added.

a. To add an option key, click **Add Option** and enter the key. Option keys can also be added post installation by going to **Administrative Tools**.

b. Click **Next**.

If no release key is entered, an evaluation version which includes support for three systems, twenty-five clients for Cisco TMS, and Cisco TMS Scheduler will be installed.For questions regarding release or option keys, contact your Cisco Reseller or Cisco Support.

2. You can now pre-configure default settings to allow Cisco TMS to immediately start working with a basic network configuration (these settings can be changed after installation). If configured correctly, Cisco TMS can automatically discover, monitor, log, provide phone books, and schedule a basic existing H.323/SIP network.
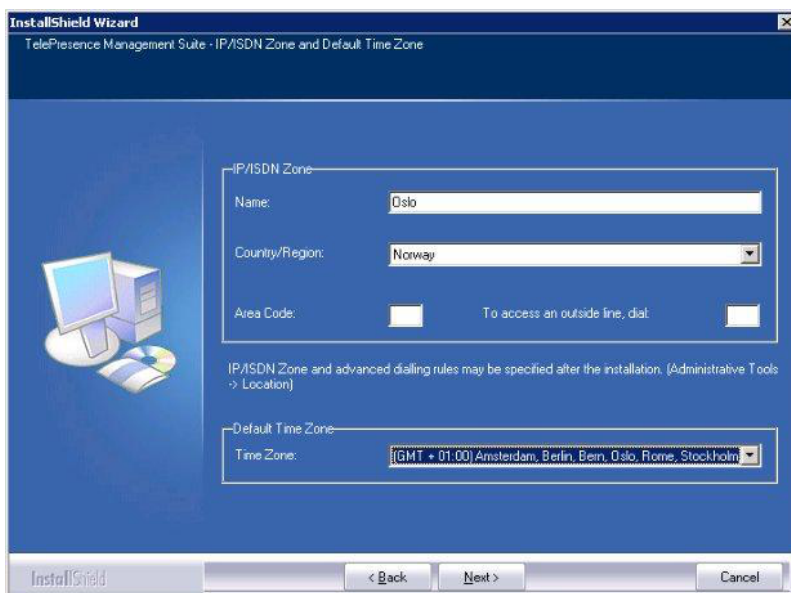

If upgrading, values from the existing database are displayed.

Field label	Description
Cisco TMS Server IP Address	The IP address of the local server.
Cisco TMS Server IPv6 Address	The IPv6 address of the local server. If IPv6 is not enabled on the Windows Server, this field can be left blank.
IP Broadcast Address […]	The broadcast address(es) for the networks that Cisco TMS is to automatically search for devices. (Systems that Cisco TMS discovers can be automatically added to Cisco TMS with their management settings added.) Multiple broadcast addresses can be entered separated by commas. Cisco TMS will search networks by sending a SNMP Discovery packet to the supplied addresses. The default value will be the broadcast address of the Cisco TMS server's network.
Enable automatic registration of systems in Cisco TMS	If enabled, systems Cisco TMS discovers on the network will automatically be added into a folder in Cisco TMS and have their management settings configured. This setting is disabled by default.
Sender E-mail Address	The email address you wish to appear in the **From** field of messages sent by Cisco TMS. Example: `videomanagement@company.com`.
SMTP Server IP Address	The network address of the SMTP server Cisco TMS will use to send email. Additional authentication configuration settings can be set up post installation as needed.

Click **Next** when done modifying the settings. Cisco TMS then contacts the supplied SMTP server to verify the settings and warns you if it was not able to contact the server.

3. The installer will now ask for zone information.

Zones are a configuration concept used by Cisco TMS to route phone numbers and aliases when scheduling calls and using phonebooks.

The information entered here creates the first IP and ISDN zones in Cisco TMS, which will be set as the initial default to allow a basic IP network to operate after installation. Additional zones and configurations must be added post installation for networks with multiple locations or more complex elements.

Field label	Description
Name	A descriptive name for the zone, normally referencing the city or building.
Country	The country this zone is located in. This is used for ISDN dialing information.
Area Code	The area code for the location, if applicable. This is used for ISDN dialing information
To access an outside line, dial	The prefix to reach an outside line on your ISDN circuits, if applicable.
Default Time Zone	Default timezone for new systems and users. Specific settings for each user or device can be added and modified later.

When done modifying the settings, click **Next**.

4. Verify all the settings in the displayed summary and click **Next**.
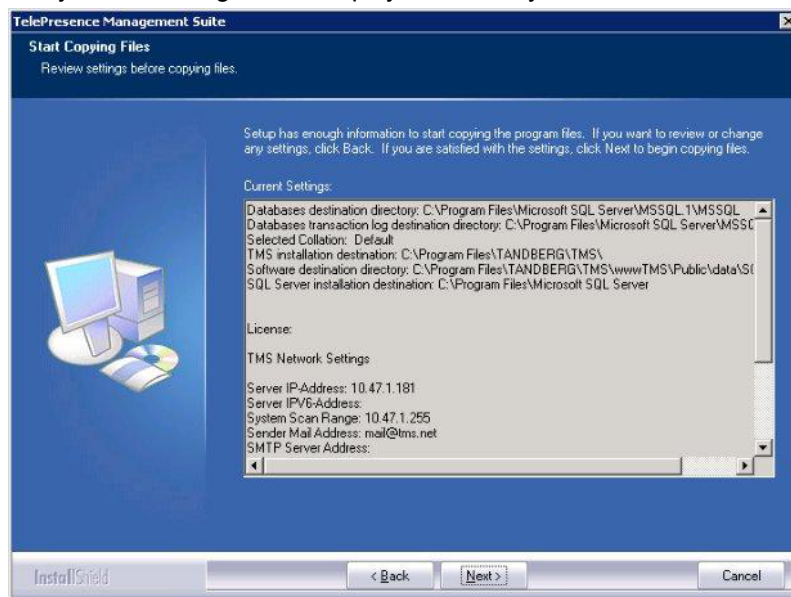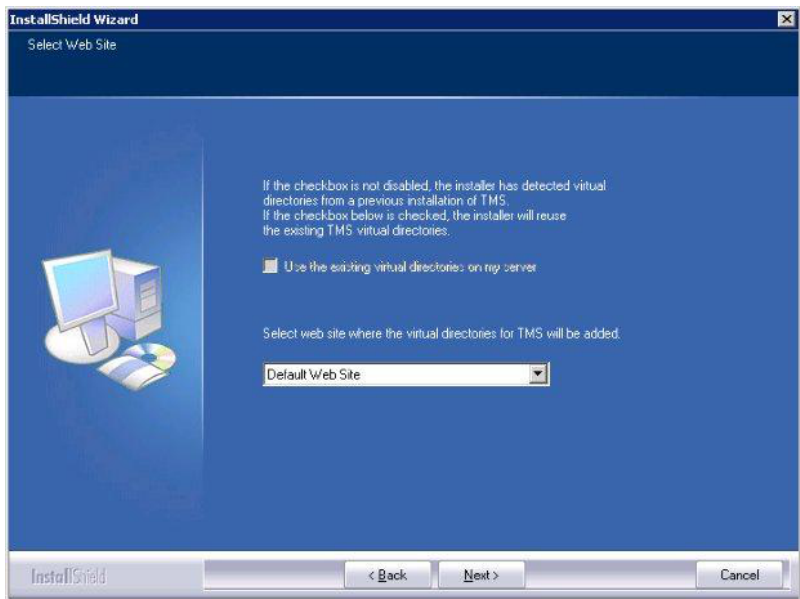
"Custom" installation

Follow the steps in this section if you chose the *Custom* setup type during Initial installation.

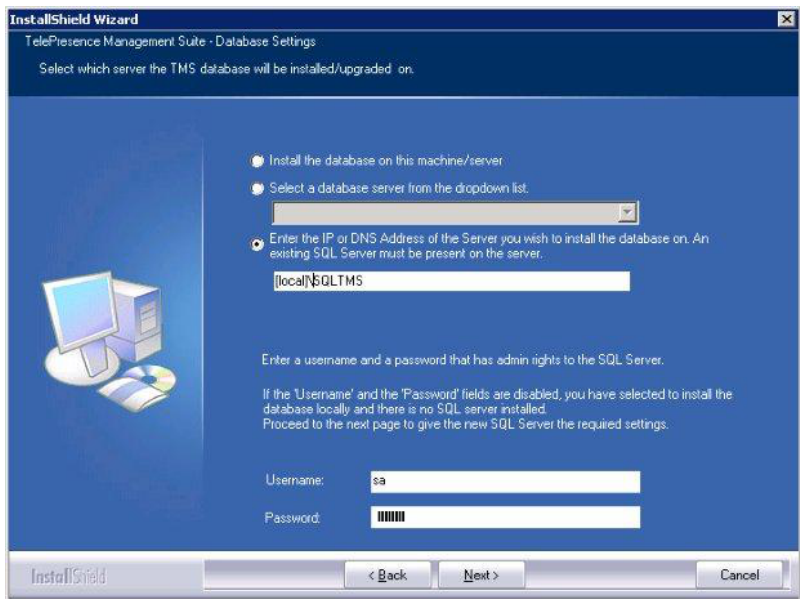## Selecting components and database options

1. Choose which components to install and click **Next**. Deselecting Cisco TMS means that only SQL Server 2008 Express Edition and the Cisco TMS database, if needed, will be installed.
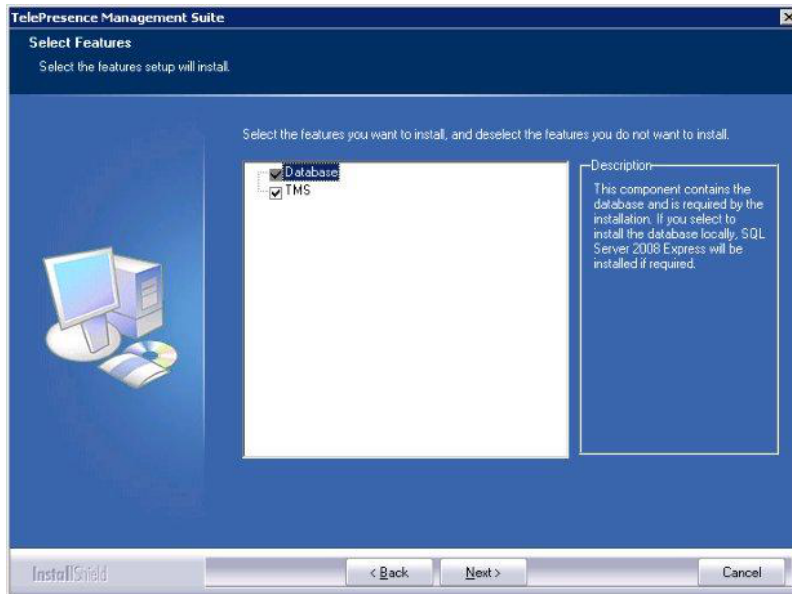
2. Select the website to install into from the drop-down menu. By default Cisco TMS installs itself by creating a virtual directory in the Default website. The installer detects previously used Cisco TMS virtual directories within the IIS server. If you wish to reuse them, select *Use the existing virtual directories on my server* . If there are no existing virtual directories used by Cisco TMS on the server, this option is unavailable.
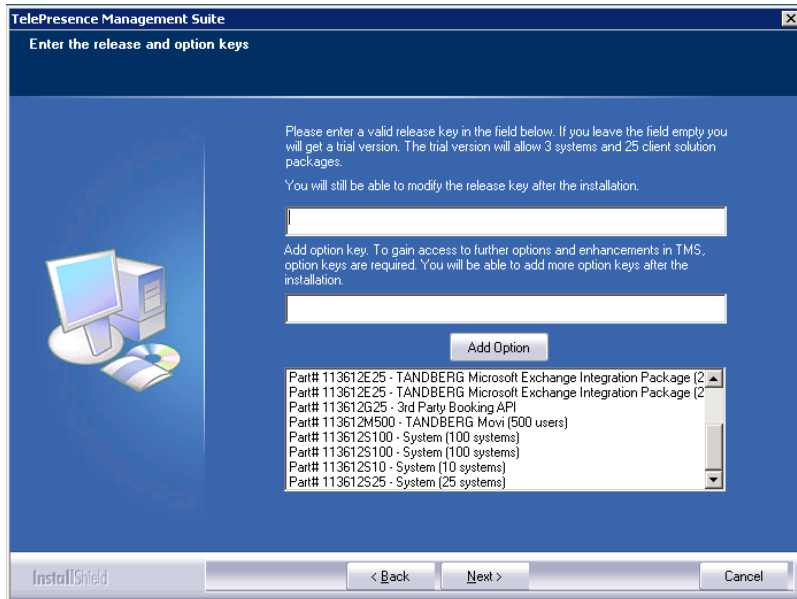
3. Supply the required database settings.

Field	Description
Install Database on this machine…	Select this option to install the database on a SQL Server on the local server. If the installer finds an existing installation, the name of the instance is displayed. At the bottom of the screen enter the SQL Login and password to use. If no local install is found, selecting this option installs a new named instance of SQL Server 2008 Express Edition.
Select a database server from…	To install on an existing remote SQL server, select the server from the drop-down list of existing SQL servers.

Enter the IP or DNS Address of the Server…	Use this option to install the Cisco TMS database on an existing remote SQL Server if the server is not listed in the drop-down list. Use the standard Microsoft SQL conventions to specify named instances, for example: `sql1.company.com\vidgrp`. If you are unsure of what to enter for your existing SQL server, ask your SQL Server Administrator.
Username/Password	If you selected an existing SQL Server above, enter the SQL Login information. The specified user is used to create and/or access the Cisco TMS database. If you are installing a new SQL Server locally, these fields are disabled and a new dialog is displayed after you click **Next** in which you must set a new SA password for the database server.

4. If an existing Cisco TMS database is found on the specified SQL server, a prompt asks whether you want to re-use the existing database. If the database is an older version and you select *Yes*, Cisco TMS automatically updates the existing database to the current version and retains the existing information. If you choose *No*, the installer quits and you must manually remove the database from the SQL server if you wish to use that SQL Server. Read Upgrading From a Previous Cisco TMS Version before proceeding with an upgrade to ensure you are prepared for any additional steps or changes that must be performed based on your previous Cisco TMS version.
5. We recommend that you back up the database before it is upgraded.
   - The backup is optional. To skip it, click **Next**.
   - To perform the backup:
     i. Enter a path for the backup file and filename, or click **Browse** to navigate to a folder. The backup is done on the SQL Server itself, so these values are local to the SQL Server.
     ii. Click **Backup** to start the backup.
     iii. When the backup is complete (this may take several minutes), click **Next**.

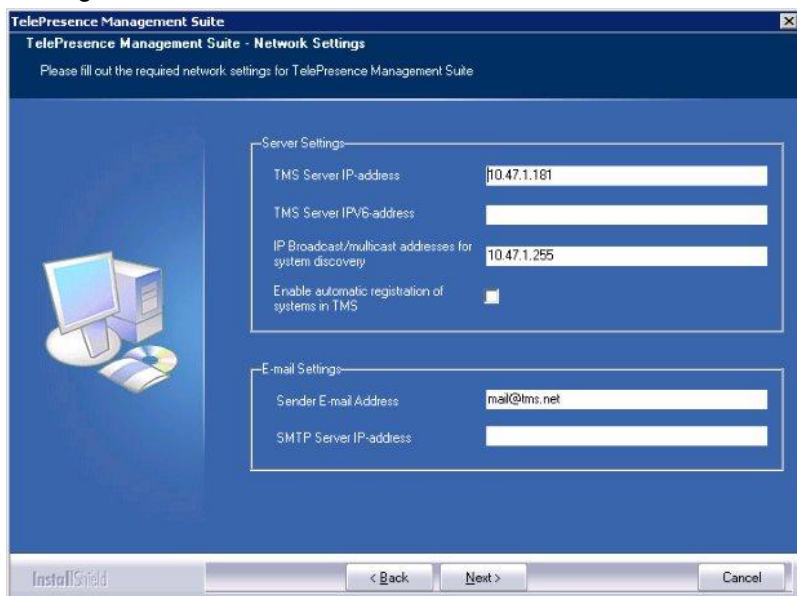# Activating and pre-configuring the installation

1. The **Release and option keys** dialog is now displayed and any existing keys are shown if upgrading. Enter the key(s) to enable additional systems, extensions, or features. A new release key is also required when upgrading to a new major release. The release key must be entered before adding option keys, which are validated as they are added.

a. To add an option key, click **Add Option** and enter the key. Option keys can also be added post installation by going to **Administrative Tools**.

b. Click **Next**.

   If no release key is entered, an evaluation version which includes support for three systems, twenty-five clients for Cisco TMS, and Cisco TMS Scheduler will be installed.For questions regarding release or option keys, contact your Cisco Reseller or Cisco Support.

2. You can now pre-configure default settings to allow Cisco TMS to immediately start working with a basic network configuration (these settings can be changed after installation). If configured correctly, Cisco TMS can automatically discover, monitor, log, provide phone books, and schedule a basic existing H.323/SIP network.
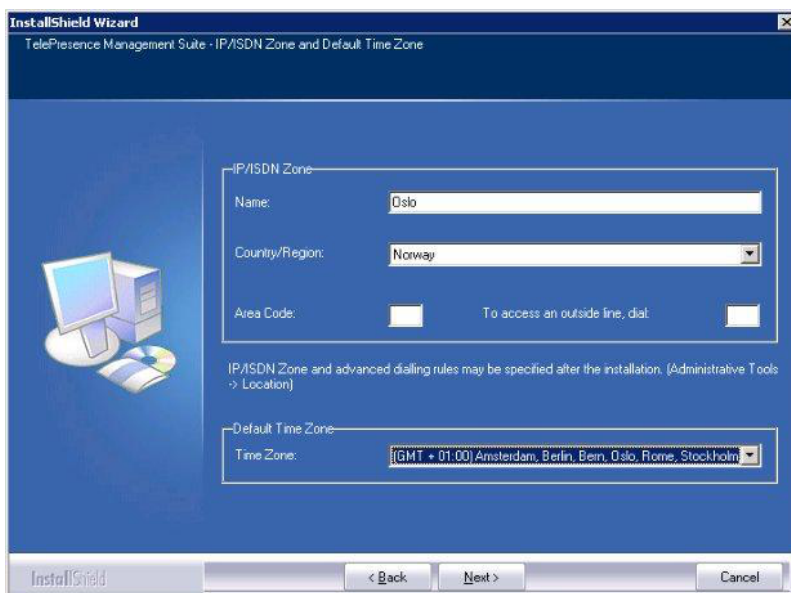

If upgrading, values from the existing database are displayed.

Field label	Description
Cisco TMS Server IP Address	The IP address of the local server.
Cisco TMS Server IPv6 Address	The IPv6 address of the local server. If IPv6 is not enabled on the Windows Server, this field can be left blank.
IP Broadcast Address […]	The broadcast address(es) for the networks that Cisco TMS is to automatically search for devices. (Systems that Cisco TMS discovers can be automatically added to Cisco TMS with their management settings added.) Multiple broadcast addresses can be entered separated by commas. Cisco TMS will search networks by sending a SNMP Discovery packet to the supplied addresses. The default value will be the broadcast address of the Cisco TMS server's network.
Enable automatic registration of systems in Cisco TMS	If enabled, systems Cisco TMS discovers on the network will automatically be added into a folder in Cisco TMS and have their management settings configured. This setting is disabled by default.
Sender E-mail Address	The email address you wish to appear in the **From** field of messages sent by Cisco TMS. Example: `videomanagement@company.com`.
SMTP Server IP Address	The network address of the SMTP server Cisco TMS will use to send email. Additional authentication configuration settings can be set up post installation as needed.

Click **Next** when done modifying the settings. Cisco TMS then contacts the supplied SMTP server to verify the settings and warns you if it was not able to contact the server.

3. The installer will now ask for zone information.

Zones are a configuration concept used by Cisco TMS to route phone numbers and aliases when scheduling calls and using phonebooks.

The information entered here creates the first IP and ISDN zones in Cisco TMS, which will be set as the initial default to allow a basic IP network to operate after installation. Additional zones and configurations must be added post installation for networks with multiple locations or more complex elements.

Field label	Description
Name	A descriptive name for the zone, normally referencing the city or building.
Country	The country this zone is located in. This is used for ISDN dialing information.
Area Code	The area code for the location, if applicable. This is used for ISDN dialing information
To access an outside line, dial	The prefix to reach an outside line on your ISDN circuits, if applicable.
Default Time Zone	Default timezone for new systems and users. Specific settings for each user or device can be added and modified later.

When done modifying the settings, click **Next**.

4. The next screen allows you to specify installation paths and directories to use for the installation. Fields that cannot be modified because the software is already installed are disabled/grayed out.
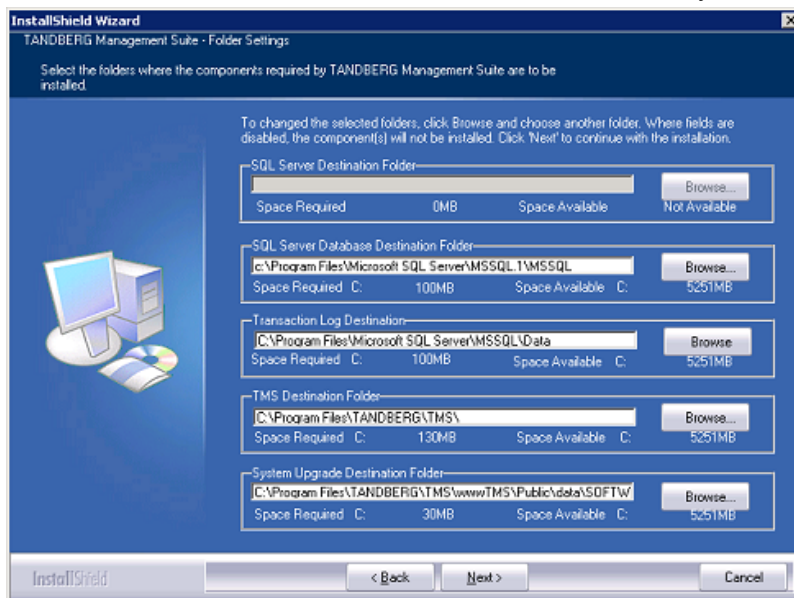
5. Verify all the settings in the displayed summary and click **Next**.
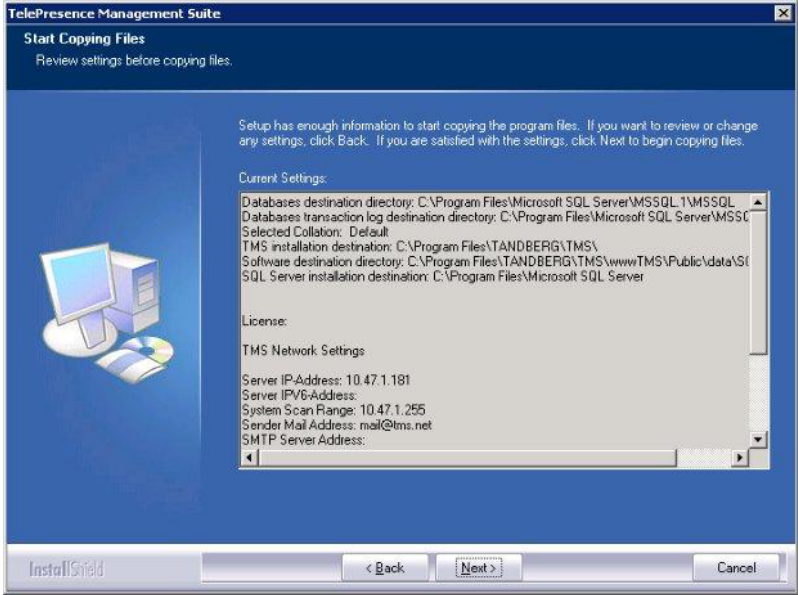
Setting up Cisco TelePresence Management Server

Cisco TelePresence Management Server is Cisco-provided server hardware that is delivered with the Cisco TelePresence Management Suite software pre-installed. The server is intended for small to medium-sized networks (up to 100 managed systems).

This section covers the following topics:

- Operator safety summary. For your safety, read before operating the server.
- Installation precautions and hardware compliances : preparing the installation site and connecting the cables.
- Using the LCD panel : operating the server panel and using it to configure the IP address.
- Configuring the server OS: using the Microsoft Server web interface for basic configuration settings.
- Operating, maintaining, and upgrading the server

Operator safety summary

Carefully observe all warnings, precautions and instructions when operating the equipment.

Equipment markings

The lightning flash symbol within an equilateral triangle is intended to alert the user to the presence of uninsulated dangerous voltages within the product's enclosure that may be of sufficient magnitude to constitute a risk of electrical shock.

The exclamation mark within an equilateral triangle is intended to alert the user to the presence of important operating and maintenance/servicing instructions accompanying the equipment.

RISK OF FIRE— REPLACE FUSE AS MARKED

0.5A 250V

WARNING: TO REDUCE THE RISK OF FIRE OR ELECTRIC SHOCK, DO NOT EXPOSE THIS DEVICE TO RAIN OR MOISTURE.

CAUTION
RISK OF ELECTRIC SHOCK
DO NOT OPEN

Warnings

- Water and moisture: Do not operate apparatus under or near water—for example near a bathtub, kitchen sink, or laundry tub, in a wet basement, or near a swimming pool or in areas with high humidity.
- Cleaning: Unplug apparatus from wall outlet before cleaning or polishing. Do not use liquid cleaners or aerosol cleaners. Use a lint-free cloth lightly moistened with water for cleaning the exterior of the apparatus.
- Ventilation: Do not block any of the ventilation openings of the apparatus. Install in accordance with instructions. Never cover the slots and openings with a cloth or other material. Never install the apparatus near heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.
- Grounding or polarization: Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding-type plug has two blades and a third grounding prong. The wide blade or third prong is provided for your safety. If the provided plug does not fit into your outlet, consult an electrician.
- Power-cord protection: Route power cord to avoid it being walked on or pinched by items placed upon or against it, paying particular attention to the plugs, receptacles, and the point where the cord exits from the apparatus.
- Attachments: Only use attachments as recommended by the manufacturer.
- Accessories: Most systems should only be used with a cart, stand, tripod, bracket, or table specified by the manufacturer, or sold with the apparatus. When a cart is used, use caution when moving cart/apparatus combination to avoid injury from tip-over.
- Lightning: Unplug apparatus during lightning storms or when unused for long periods of time.
- Servicing: Do not attempt to service the apparatus yourself as opening or removing covers may expose you to dangerous voltages or other hazards, and will void the warranty. Refer all servicing to qualified service personnel.

- Damaged equipment: Unplug apparatus from outlet and refer servicing to qualified personnel under the following conditions:
  - when power cord or plug is damaged or frayed
  - if liquid has been spilled or objects have fallen into the apparatus
  - if apparatus has been exposed to rain or moisture
  - if apparatus has been dropped and subjected to excessive shock, or cabinet has been damaged
  - if apparatus fails to operate in accordance with the operating instructions

Installation precautions and hardware compliances

Safety precautions:

- Never install communication wiring during a lightning storm.
- Never install jacks for communication cables in wet locations unless the jack is specifically designed for wet locations.
- Never touch uninstalled communication wires or terminals unless the communication line has been disconnected at the network interface.
- Use caution when installing or modifying communication lines.
- Avoid using communication equipment (other than a cordless type) during an electrical storm. There may be a remote risk of electrical shock from lightning.
- Do not use the communication equipment to report a gas leak in the vicinity of the leak.
- Always connect the product to an earthed socket outlet.
- The socket outlet must be installed near to the equipment and be easily accessible.
- Switch the power OFF before installing cables.

This product complies with the following directives:

- LVD 73/23/EC, EMC 89/366/EEC, R&TTE 99/5/EEC,
- Directive 73/23/EEC (Low Voltage Directive)
- Standard EN 60950-1
- Directive 89/336/EEC (EMC Directive)
- Standard EN 55022, Class A
- Standard EN 55024
- Standard EN 61000-3-2/-3-3
- Approved according to UL 60950-1 and CAN/CSA C22.2 No. 60950-1-03
- Complies with FCC15B Class A

Unpacking

To avoid damage to the unit during transportation, Cisco TelePresence Management Server is delivered in a special shipping box, which contains the following components:

- Rack-ears, screws and screwdriver.
- Cables:
  - Power cable
  - Ethernet cable
  - Cisco TelePresence Management Server

Installation site preparations

- Make sure that Cisco TelePresence Management Server is accessible and that all cables can be easily connected.
- For ventilation leave a space of at least 10 cm (4 inches) behind the rear panel and 10 cm (4 inches) in front of the front panel.

- The room in which you install Cisco TelePresence Management Server should have an ambient temperature between 0°C and 35°C (32°F and 95°F) and between 10% and 90% non-condensing relative humidity.
- Do not place heavy objects directly on top of the server.
- Do not place hot objects directly on top, or directly beneath the server.
- Use a grounded AC power outlet.

Rack mounting

Note: The following procedure is optional.

Cisco TelePresence Management Server comes with rubber feet for standalone installation and brackets for mounting in standard 19" racks.

Before starting the rack mounting, ensure that Cisco TelePresence Management Server is placed securely on a hard flat surface.

1. Disconnect the AC power cable.
2. Set up the mounting space in accordance with the site preparations described above.
3. Attach the brackets to Cisco TelePresence Management Server on both sides of the unit using the 8 screws that are provided.
4. Insert Cisco TelePresence Management Server into a 19" rack, and secure it at the front using four screws.
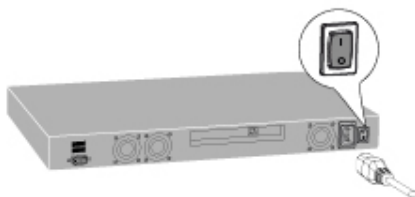
Connecting the cables

LAN cable

Connect a LAN cable from the "LAN 1" connector on Cisco TelePresence Management Server to your network. The LAN 2, 3 and 4 connectors are not used and should be left open.

Power cable

Connect the system power cable to an electrical distribution socket. Press the power switch button at the back to *1*. The power indicator LED, marked `Pwr`, on the front panel lights up.

Shutting down

Cisco TelePresence Management Server must be shut down via the front LCD panel or from the Windows interface before powering the unit off.

Connecting a monitor and keyboard

Initial network configuration is done using the LCD Panel. If direct access to the server is subsequently required, you can connect a VGA monitor, USB keyboard and mouse to access the server console.

Using the LCD panel

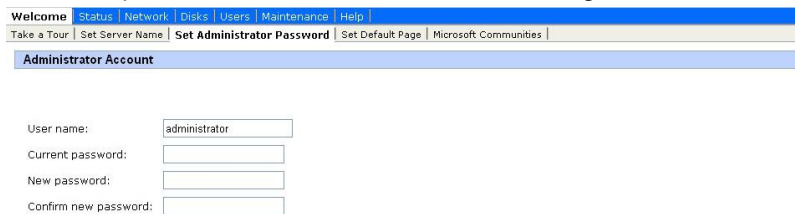|		
	Up and Down arrows	Used to select items in the menu, move between values in a numerical address and modify numerical values.
	Enter	Used to enter edit mode and confirm a selection or entry.
	Return	Used to return to the previous menu or exit edit mode without saving the latest entry.

Configuring the IP Address setting

Cisco TelePresence Management Server requires an IP Address before it can be used, and this is done using the LCD panel.

1. Power up the server and wait for it to finish booting. The LCD Panel should show the server's current IP after the server has finished starting up.
2. Press **Enter** to display the Main Menu.
3. Use the Up or Down arrow to select **IP Settings**.
4. Press **Enter** to confirm your selection.
5. Use the **Up** or **Down** arrow to select **IP Address** and press **Enter** twice to enter edit mode.
6. Moving between characters using the Up and Down arrows, edit the values by pressing **Enter** and using the **Up** or **Down** arrow to modify the value. Press **Enter** again to confirm the value, or press **Return** to restore the previous value.
7. When you have finished editing the address, press Return. At the Save Changes? prompt, use the **Up** or **Down** arrow to select **Yes** and press **Enter**.
8. Press **Return** to go back to the **IP Settings** menu.
9. Use the **Up** or **Down** arrow to select **Subnet Mask** and press **Enter** twice.
10. Repeat steps 5-6 to enter the Subnet Mask address.
11. Press Return to go back to the **IP Settings** menu.
12. Use the **Up** or **Down** arrow to select **Default Gateway** and press **Enter** twice.
13. Repeat steps 5-6 to enter the Default Gateway address.

Configuring the server OS

To complete the physical installation of the server, several basic server OS settings must be configured using the web interface for Microsoft Server. The following steps must be completed from another computer on the network that has Internet Explorer (ActiveX required) installed and network access to the Cisco TelePresence Management Server.

1. In the web browser URL field enter **https://<ManagementServerIPAddress>:8098** where <ManagementServerIPAddress> is the IP address of the Cisco TelePresence Management Server that you configured previously.
2. If you see a security warning stating "There is a problem with this web site's security certificate" – this is normal because your browser does not trust the default server certificate that is pre-installed. Click **Continue to this website**.
3. When prompted, enter the username Administrator and password TANDBERG.
4. Change the default administrator password:
   a. Go to **Welcome > Set Administrator Password**.
   b. Set a new password and click **OK** to save the changes.

   c. When the change is confirmed, click **OK** to return to the Welcome Screen.
   The default password for the administrator account is TANDBERG. This account has full access to the Windows Server operating system: therefore assign it a strong, secure password.

   CAUTION: Do not lose your administrator password.Cisco cannot recover lost passwords. You will need to return the Cisco TelePresence Management Server to the factory for repair and all customer data will be lost.

5. Set the Server Time and Time Zone:
   a. Go to **Maintenance > Date/Time**.
   b. Update the Time, Date, and Time Zone settings.
   c. Click **OK**.
6. Go to **Welcome > Set Server Name**, configure the server's name and Domain membership and click **OK**.

Joining the server to an Active Directory domain will simplify user administration by allowing all users in Active Directory to use their existing Windows credentials to access Cisco TMS. Enter a domain username and password authorized to join the server to the domain.

Caution: Be aware of any group policies that your Active Directory may automatically apply to servers joined to its domains. High security policies that interfere with web server operations may interfere with Cisco TMS operation.

7. Restart the server to complete any changes to the computer name or domain membership.
8. Ensure that any available security updates are installed (see Operating, maintaining, and upgrading the server).

Operating, maintaining, and upgrading the server

Cisco TelePresence Management Server is a Cisco-maintained "black-box" server designed to be operated using the LCD panel or web interface, while operation and management of the Cisco TMS software application is performed solely using the Cisco TMS web interface. Access to the server's operating system is available via local console connections or Microsoft Remote Desktop Client, but it is not required for normal operations.

As with all servers, the server hardware should be housed in a secure space and not be accessible to non-administrators. The server should remain on at all times for normal operation.

When delivered, the operating system is "locked down" and hardened following Microsoft's security recommendations for a server of this type. The server does not allow any remote connections except where necessary for Cisco TMS communication with users and the devices that it manages. The SQL database and other internal components are not accessible remotely. Cisco recommends that you do not modify any of the operating system's underlying settings.

Starting and stopping the server

Cisco TelePresence Management Server can be restarted and shut down via the LCD panel. As with all servers, it should not be powered off abruptly and restarts/shutdowns should always be performed via the software controls rather than the power switch - unless the server itself and the LCD panel are unresponsive. After a full shutdown, it is safe to turn off the power switch.

To start up the Cisco TelePresence Management Server:

1. Connect the power.
2. Turn the power switch to *1* (on).

When the start up process nears completion, the LCD panel will show the server's current IP address .

To restart or shut down from the LCD panel:

1. Press **Enter** to display the **Main Menu**.
2. Use the **Up** or **Down** arrow to select **Commands** and press **Enter** .
3. Take one of the following actions:
   - Use the **Up** or **Down** arrow to select *Restart* and press **Enter**.
   - Use the **Up** or **Down** arrow to select *Shutdown* and press **Enter**.
4. At the confirmation prompt, use the **Up** or **Down** arrow to select *Yes* and press **Enter**.

The server can safely be powered off after a few minutes. There is no specific feedback on the LCD panel that the shutdown process has completed.

The system can also be reset or shut down using Windows Remote Desktop or the web interface:

1. Start a web browser and enter the address https://<ManagementServerIPAddress>:8098 where <ManagementServerIPAddress> is the IP address of Cisco TelePresence Management Server.
2. If you see a security warning stating "There is a problem with this website's security certificate" – this is because your browser does not trust the default server certificate installed. Click **'Continue to this website'** to acknowledge the warning and continue.

3. When prompted, enter the administrator username and password.
4. Select the **Maintenance** tab. Click **Shutdown**, then opt to either shut down or restart the server.

Performing database backups

Cisco TMS stores all its customer data in its SQL database named **tmsng**.

Follow best practices and take regular backups of the database to ensure that you can recover and restore the system in case of a system failure or as part of a larger disaster recovery plan.

Additional help on performing SQL backups is available in the *Cisco TMS Database Knowledge Tips* document. Backups should be stored away from the Cisco TMS server for maximum protection.

TMS Agent database backup

To perform a backup of the TMS Agent database, go to **Administrative Tools > Configuration > TMS Agent Settings**. The installer automatically places the provisioning database (OpenDS) backup in the Cisco TMS backup folder (by default, **<TMS folder>\wwwTMS\Data\Backup\opends**).

Also note that Cisco TelePresence Management Server is delivered with remote SQL access disabled. If you enable remote access to the SQL Server for backup purposes, be sure to change the SQL sa password from the default password. If you change the SQL password, update TMS Database Connection properties using the TMS Tools application installed in the TANDBERG Program Group on the Cisco TelePresence Management Server.

Operating system updates

When delivered, the Automatic Updates functionality of Microsoft Windows is turned off. This is by design to avoid any untested changes to the underlying operating system. To keep the operating system current and secure, Cisco provides regular security updates as self-contained installers for the Management Server. These updates are distributed as Cisco TelePresence Management Server security updates and are made available to customers via the web site:

http://www.tandberg.com/support/tandberg_device_security.jsp and http://ftp.tandberg.com

Cisco strives to make these security updates available in a timely fashion because Microsoft releases its own monthly security updates.

Note: It is important that you download and install all security updates from the FTP site before using this product. Also check this site regularly to see whether new security updates are available. Normally, updates are available on a monthly basis or as required.

Software installation and upgrades on the Cisco TelePresence Management Server

The Cisco TelePresence Management Server is upgraded using the same software (and therefore the same steps) used for software-only installations of Cisco TMS. The Cisco TMS installer automatically detects if the software is being run on Cisco TelePresence Management Server and acts accordingly.

To perform a Cisco TMS upgrade:

1. Using the Microsoft Remote Desktop client, connect to the Cisco TelePresence Management Server's IP or hostname.
2. Log in using the local administrator username and password.
3. Copy the Cisco TMS software installer to the Cisco TelePresence Management Server using a file share, web download, or the drive mapping feature of Remote Desktop Client.
4. Follow the steps in the Installing or upgrading Cisco TMS section of this document, following the path for the "Complete" installation choice.

Note:: The SQL Server sa login information needed during the upgrade the default for the SQL Login is username: sa and password: TANDBERG.

Security policy

The Cisco TelePresence Management Server's security policy is updated and maintained by the Cisco TMS installer. If an administrator makes changes to negate any of these security lockdown steps, the security policy will be re-applied automatically the next time the Cisco TMS software installer runs.

Getting started with Cisco TMS

This section provides guidance on initial access to and setup of Cisco TMS:

- Accessing Cisco TMS for the first time: locating and signing in to Cisco TMS.
- Web page features and layout: a brief overview of how the web interface works.
- Setting up Cisco TMS: how to configure a baseline setup.
- Working with phone books: giving users access to the contacts they need.
- Adding and managing systems: how to get started organizing, adding, and managing systems.
- Creating a scheduled conference: how to create, edit, and monitor conferences in Cisco TMS.
- Reporting : how Cisco TMS makes conference statistics available.

Accessing Cisco TMS for the first time

Once Cisco TMS is installed, it is only accessed using a web browser:

1. Do one of the following:
   - Use the shortcut provided in the Cisco program group in the Start menu.
   - Enter `http://<serveraddress>/tms` in your web browser's URL field, where <serveraddress> is the hostname (recommended) or IP address of your server. Using the hostname accommodates integrated authentication with Active Directory.
2. If accessing the website from the server console, you will usually authenticate automatically with your currently logged in username and Cisco TMS will open. If not, you will be asked for authentication details.
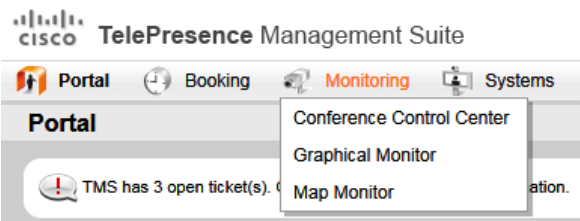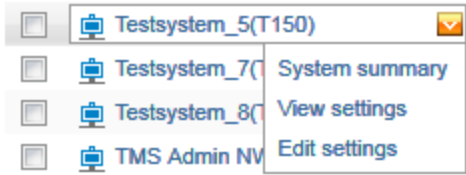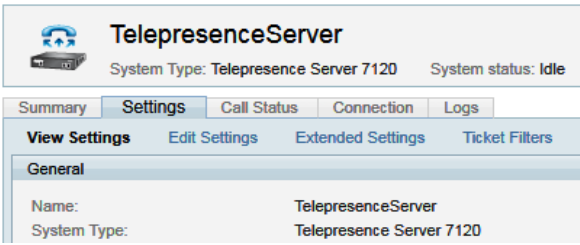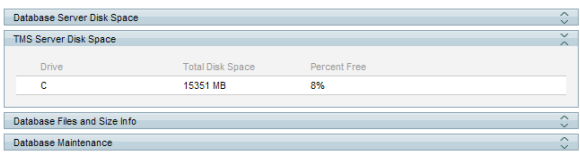
   Most browsers will display two fields in the login window that appears—a username and password field. How you enter your username will depend on the type of Windows account you are using.

Field	Description	Example
Domain Users	Username should be entered as domain\username. The username@<Domain DNS name> format is also suitable, but less commonly used.	corp\joe.smith
Local Windows Accounts	Username should be entered as machinename\username	tms-2\administrator

3. A user profile window should pop up after you successfully authenticate. If not, look for pop-up blocking alerts from your browser, and disable pop-up blocking for the Cisco TMS.
4. Fill in the details of the user profile and click **Update Your Personal Information**.

Web page features and layout

Being the first user to sign into Cisco TMS, you are automatically an administrator and have full access to Cisco TMS. Users with restricted permissions will not see or have access to all menus and options.

User interface element	Image	Description
Top-level menu		The Cisco TMS functionality is grouped by main categories in a top menu. Hover the menu items to expand each sub-menu.
Drop-down menus		Hovering over items in a list will display an orange drop-down menu icon when available.
Lists		The sorting of most lists in Cisco TMS can be changed by clicking the title of the column you want the list sorted by. A small triangle next to the column title will indicate whether the sorting is ascending or descending. Some lists may have hundreds or even thousands of entries. Rather than show them all in a single list, most lists in Cisco TMS are split into pages with **Previous** and **Next** links at the bottom
Tabs		Many pages in Cisco TMS have multiple views available, shown as tabs across the top. There can be multiple levels of tabs. In the screenshot to the left, there are multiple pages/views available, including Summary, Settings, Call Status, Connection, and logs. The active tab is displayed in a darker blue and has additional views under it. The current view is highlighted.
Panels		Each panel has a blue bar at the top. If the bar has arrow icons at the right edge, clicking on the blue bar will cause the panel to either collapse or expand. This allows you to choose which areas of the screen to concentrate on or see more of.

User interface element	Image	Description
Search field	Search...	Use the search box at the top right of every page to find an individual telepresence system by name, phone number, serial numbers, or other property.
Help	(?)	The help icon takes you to context-sensitive help for the page you are on.
Log out	O→	The key icon logs you out of Cisco TMS.

Setting up Cisco TMS

Cisco TMS is designed to automate as much of the configuration of the system as possible and will function for a basic telepresence network right out of the box.

This baseline configuration is only a starting point, and is not intended to be the final configuration of Cisco TMS. As an administrator you will want to tune Cisco TMS's default behaviors to suit your organization's needs, set up permissions for various users, and configure Cisco TMS's network model so that all conference handling functionalities will be available.

Using configuration templates

A common administrative need is to apply a common group of settings to one or more systems. Configuration templates in Cisco TMS allow you to define a set of configuration parameters to be applied to systems. The template can include configuration choices for different system types, and Cisco TMS will only apply the settings that relate to the individual system being updated.

Administrators can define multiple templates, and may choose to apply them

- manually per system
- automatically as systems are added to Cisco TMS
- persistently every time the system is powered up

As part of the default installation, Cisco TMS created a template for you named "Discovered Systems Template", containing a group of settings that are automatically applied to all systems automatically added to Cisco TMS by System Discovery.

This was done via the Default Configuration template for Discovered Systems setting under **Administrative Tools > Configuration > Network Settings**. This topic will review this default as a working example of how to use Configuration Templates.

Editing a template

1. Open **Systems > Provisioning > Configuration templates**.
2. Click on the template titled "Discovered Systems Template".
3. The **Type** for the settings in this template is *Other type* because they are Cisco TMS configuration settings, not configuration options from the device's commands itself.
4. Click **Edit** to see the **Edit Settings** page. All templates have some common Cisco TMS settings added to them to start with, such as **Zones** and **Phone books**.
5. To add more settings to the template, click on the **Select Advanced Settings** tab. To see a list of all available settings, simply leave the Filter box blank and the drop down set to *All Systems* and click **Search**. From this view, you can chose from all the template settings available in Cisco TMS and add them to the list to be shown on the **Template Settings** tab.
6. Add or remove settings to the template by marking a setting's check box and using the < > buttons to add or remove it from the list on the right.
7. Once the desired changes have been made, click on the **Template Settings** tab to return to the previous view.

8. On the **Template Settings** tab, enable or disable individual settings with their check boxes and set the values to use for each setting.
9. When finished, click **Save**.

Creating a new template

1. To create a new template, click the New Configuration Template button at the bottom of the Configuration Templates page at **Systems > Provisioning > Configuration Templates**.
2. Enter a name for the template.
3. Add/remove settings as described above.
4. Click **Save**.

Applying templates to systems

A template can be applied to one or many systems at once. Templates can alsobe used in more advanced features such as Persistent Settings and Automatic System Discovery.

To apply a template to a group of systems:

1. Go to **Systems > Provisioning > Configuration Templates**.
2. Hover your mouse over the template name you wish to use, and click the orange arrow to access the drop down menu. Click **Set on Systems**.
3. Select a system by clicking on it. Multiple systems can be selected by holding the `Shift` or `Control` keys when clicking on a system. Use the **< >** buttons to add and remove systems.
4. Click **Set on Systems** to start the task. The job of applying the template to systems will take place in the background on the Cisco TMS server.
5. You can view the status of the job on the Provisioning Activity Status page under **Systems > Provisioning**.

User accounts and profiles

To log into the Cisco TMS website, users must have a Windows username and password that the server is configured to trust. By default, any local Windows user account will work, as well as any Active Directory domain user account if the server is a member of an Active Directory domain.

For each user that successfully logs into Cisco TMS, it creates a user profile based on their Windows username. User passwords are not stored in Cisco TMS, existing Windows passwords are used, and if their Windows password is updated, they must use that updated password when logging into Cisco TMS.

While it is possible to create a user profile in Cisco TMS manually, this does not create a Windows user account, and deleting a user profile in Cisco TMS does not alter the user's actual Windows user account.

User profile page

Four personal information fields are mandatory:

- Windows username
- First name
- Last name
- Email address

If these are not filled in, the user will be prompted to complete them on first sign-in.

Language setting

Each user can choose their own language to use within the Cisco TMS Application. The drop-down list includes all the supported languages in Cisco TMS.

While all languages are supported in the Cisco Scheduler and notifications, a smaller subset is supported for the main Cisco TMS web interface:

- English
- French
- Russian
- Japanese
- Chinese (Simplified)
- Korean

If another language is selected, that user will see English when browsing pages that do not support their language selection.

WebEx integration

For WebEx booking to work, the booking user must have a WebEx username and password defined as their **Web Conference Username** and **Web Conference Password** in their Cisco TMS profile. This ensures that the correct user "owns" the meeting in WebEx and can log in and operate the WebEx conference.

The remaining fields are not mandatory, but are used for other Cisco TMS features. Later, if you are using Active Directory, you can configure Cisco TMS to populate these fields automatically for new users.

Configuring an initial permissions setup

For initial setup, a baseline of permissions must be established. Creating and assigning all groups can wait until you settle on a more complete and formal configuration. The permissions can be changed at any time, but it is advisable that administrators start planning from the beginning how access will be controlled in Cisco TMS and what features users will have access to by default.

It is best practice to follow the below steps to:

- Make sure that new users will not automatically have administrator rights.
- Create a default group for new users with the desired baseline permissions.

1. Create a new group to use for all your trusted users:
   a. Go to **Administrative Tools > User Administration > Groups**.
   b. Click **New** to create a new group.

   c. Name your new group as desired. For example, "All company users".

   d. Click **Save**.

2. Assign the default permissions you want all Cisco TMS users to have to the new group:

   a. Click on the Group Name in the Edit Group listing.

   b. Click **Set Permissions**.

   c. Select the check box for each permission you wish group members to have. For a starting point that gives users full access except to Cisco TMS configuration, select all the boxes except those under **Administrative Tools**. Use the check boxes in the blue title bars to mark or clear all check boxes in that section.

   d. Click **Save**.

3. Change the Default Groups:

   a. Go to **Administrative Tools > User Administration > Default Groups**.

   b. Clear all the check boxes except **Users** and your new group.

   c. Click **Save**.

   d. Any person who logs into Cisco TMS will now automatically be added to your new group, and given the permissions that group has.

4. Change the Default System Permissions:

   a. Go to **Administrative Tools > User Administration > Default System Permissions**.

   b. Clear all the check boxes for the **Users** group, and assign the permissions you would like for the new user group.

   c. Click **Save**.

5. Ensure only intended users have Site Admin access:

   a. Go to **Administrative Tools > User Administration > Groups**.

   b. Click on the **Site Administrators** group and click **Edit**.

   c. In the Members list, ensure only the users you wish to have administrator rights are listed. If any other accounts are listed, select the check box of their row and click **Remove**.

   d. Click **Save**.

Beyond initial configuration, administrators must plan their Cisco TMS deployment in terms of who needs permissions to perform what in Cisco TMS. This is controlled through

- group membership
- group permissions
- system permissions

Defining permissions and groups

Cisco TMS gives administrators the ability to control which features users have access to, such as booking, managing systems, and so on. As an administrator you also control for which systems users have access to those features. For example, this makes it possible to allow the IT team in Chicago to fully control and manage endpoints in Chicago, while preventing them from scheduling or making changes to systems in London.

When a user does not have permissions for something in Cisco TMS, it is normally hidden from their view. If they have no permissions for a system, the system will not even show in their listings. If a user has no Booking permissions, the Booking menu is not displayed. This creates very simple interfaces for users with limited roles.

You control permissions in Cisco TMS by defining User Groups and assigning users to groups. A user's permissions are the *cumulative* permissions of all groups that user is a member of, that is, the sum of the permissions for all those groups.

Changing group permissions

To change the permissions for a group:

1. Go to **Administrative Tools > User Administration > Groups**.
2. Click on the group's name.
3. Use the Set Permissions option.

Users and Site Administrators

Cisco TMS starts with several groups created by default, but the most important groups are these two groups:

- Users: All users are members of this group, and membership for the group cannot be edited. Any permission given to this group will beavailable to all Cisco TMS users.
- Site Administrators: Anyone who is a member of the Site Administrator group has full access to all features and systems in Cisco TMS. You can edit who is a member of the Site Administrator group, but you cannot edit its permissions, as it always has all permissions.

Administrators can and should define more groups to allow greater control of permissions in Cisco TMS.

Assigning users to groups

Which groups users belong to can be set in one of three ways:

- Editing the group itself. The **Edit Group** Page displays all current members, and by clicking the Add Members tab, you can specify which users to add to the group. A user can be a member of multiple groups. A user's groups can also be edited by editing the User under **Administrative Tools > User Administration > Users**.
- Assigning the user to a group automatically when the user's profile is created. Set a group as 'Default Group' to have it automatically added to any new user. Note that on first install, the Site Administrators group is marked as a Default Group. This means any person who logs into Cisco TMS will have a user profile created, and will automatically be added to the Site Administrators group giving them full rights to Cisco TMS. This is how you became an administrator automatically when first logging into Cisco TMS.
- Active Directory Groups. Cisco TMS lets you import existing groups from Active Directory. Active Directory group memberships are automatically updated in Cisco TMS groups when the user logs in.

System permissions

Permissions in Cisco TMS are a combination of feature permissions and system permissions:

- User Groups have permissions to control which portions/features of Cisco TMS a user has access to.
- System Permissions are used to control what a user can do to a particular system. Later, when you get to adding/editing systems, you can alter the permissions for individual systems.

Default permissions are given to a system when first added to Cisco TMS. This is controlled in **Administrative Tools > User Administration > Default System Permissions**, where you can set which permissions each group gets on newly added systems.

Reviewing and setting defaults

Most settings in Cisco TMS are configured automatically or have suitable default values for most organizations.

Below are important settings you should review and configure as part of your initial setup to ensure they meet your needs and to ease the configuration of other Cisco TMS features.

For detail on each setting, refer to the Cisco TMS help system.

General settings

Open **Administrative Tools > General Settings**. Important settings that should be reviewed at this time are listed below:

Setting	Description
System Contact/Email	When filled in, these display a Contact link on the bottom of all Cisco TMS pages so users can easily contact you for help or questions.
Enable Auditing	This setting enables Audit logging where Cisco TMS keeps detailed logs of all changes to systems, users, and other key elements of Cisco TMS. The Audit Log is accessible in the Administrative Tools Menu. This is disabled by default, but security conscious installs may want to enable it from the start. This feature will cause the Cisco TMS database to grow significantly faster.
Release Key/Option Keys	If you did not enter your release key and option key during install. You can enter them here. If attempting to upgrade from a trial version or adding new options, this is where license information is entered.

Network settings

Open **Administrative Tools > Network Settings**. Significant settings that should be reviewed at this time are listed below:

SNMP Community Name	This is a comma separated list of common SNMP strings Cisco TMS will use when discovering and adding systems to Cisco TMS. If you use a customized SNMP Community Name on your existing systems, be sure to add it to this list.
E-mail Addresses to Receive System and Network Notifications	You should enter your email address here so Cisco TMS can send you notifications about discovering non-registered endpoints, system event failures, and other administrative messages. Multiple email addresses must be comma separated.
Automatic System Discovery	This feature is enabled by default. It automatically adds systems Cisco TMS discovers to a folder in System Navigator, and configures their management properties to work with Cisco TMS. Cisco TMS configures the systems with basic settings from the "Discovered Systems Template". Modify this template to specify default settings that you wish all new systems to have.

Active Directory	These settings allow Cisco TMS to use Active Directory for its user and group settings. If the Cisco TMS server is a member of a domain, it is highly recommended you enable these settings by entering a valid Windows Domain account. The account does not need to be an administrator account, just a normal user account. If Lookup User Information… is enabled, when a new user profile is created, Cisco TMS will automatically populate as many of the fields in the user profile as possible from Active Directory. Allow AD Groups simplifies Cisco TMS Groups by allowing you to use Groups from Active Directory as Cisco TMS User Groups which automates which Cisco TMS groups a user belongs to. For further detail on AD Groups, refer to the *Cisco TelePresence Management Suite Administrator Guide*.
Scan SNMP Capable Systems to Allow Quick Discovery of Inaccessibility	This setting will allow Cisco TMS to more quickly detect whether a system has gone offline. Enabling this is recommended.
SNMP Broadcast/MultiCast Address(es)	This is the network addresses that were configured in the Cisco TMS Installer. Cisco TMS will send a SNMP query to these addresses to find new systems. If your network spans multiple networks, add the broadcast address for each, separated by commas to allow Cisco TMS to find systems automatically. Do not worry if all networks are not represented here as Systems can also be added manually and through systems contacting Cisco TMS.
Enforce Management Settings	This setting is enabled by default and should remain enabled. This setting is essential to ensure systems are properly configured to point to your Cisco TMS server.
Advanced Network Settings	To account for diverse network configurations, Cisco TMS supports the notion of two networks that can access Cisco TMS: ■ Internal LAN: this is usually the same as your organization's internal network. ■ Public Internet/Behind Firewall: you may have systems that you wish to manage outside the organization's firewall or proxy. The public hostname used should resolve to an IP forwarded to the Cisco TMS server's IP address. Each system added to Cisco TMS has a Connectivity parameter where you specify which network identity Cisco TMS should use when communicating with the system. Note that Cisco TMS is still only connected to one physical LAN port and only one IP Address. Cisco TMS does not support multihomed networking.
TMS Server IPv4/IPv6 Addresses	These were configured during installation and should be the IP addresses used to reach your Cisco TMS server.
TMS Server Fully Qualified Host Name	The fully qualified domain name used to access your Cisco TMS server from the internal, or local, network. This setting will be used with systems that support DNS and must be configured correctly. If the server has no hostname that is usable, enter the IP address that systems would use to reach Cisco TMS.
TMS Server Address (Fully Qualified Host Name or IPv4 Address):	The fully qualified domain name used to access your Cisco TMS server from an outside network, if different from the local hostname. This setting must be configured to use features such as SOHO/Behind Firewall support. If the server has no hostname that is usable, enter the IP address that systems would use to reach Cisco TMS.

Automatic Software Update	This functionality allows Cisco TMS to automatically check over a secure link for new software available for your systems, and notify you of your Service Contract status for your Cisco Systems. No personal information is sent during this communication except the system identifying information such as serial numbers and hardware identifiers. If you do not wish to have Cisco TMS check for software, you can disable this feature. If your network requires a web proxy to reach the internet, configure the properties for it here.
Secure-Only Device Communication	This is off by default and only should be enabled in specific customer scenarios. Please see *Implementing Secure Management* for more information.

Configuring hostnames for the TMS Agent

The TMS Agent application does not use the fully qualified hostname configured for the internal LAN described above. In a single Cisco TMS environment we do however recommend that they be the same. The TMS Agent uses the actual local hostname of the Cisco TMSserver, and this must match the DNS A record for the TMS Agent.

In a redundant Cisco TMS setup, the fully qualified DNS hostname configured here must be unique and resolvable to the network load balancer. DNS records for each particular redundant Cisco TMS (local hostname) must also be created, so that the TMS Agent can resolve and replicate appropriately.

Mail settings

Open **Administrative Tools > Mail Settings**. These settings were configured during the Cisco TMS installation. However, if your mail server requires SMTP Auth, specify the username and password here. The settings will be validated when you click **Save**.

General settings

Open **Administrative Tools > Conference Settings**. These settings control most of the behaviors of Cisco TMS for scheduled calls and for monitoring of active calls. Significant settings that you may wish to update are:

Default Bandwidth	This is the default bandwidth suggested for H.323 and SIP calls in Cisco TMS Scheduling.
Default ISDN Bandwidth	This is the default bandwidth suggested for ISDN calls in Cisco TMS Scheduling
Set Conferences as Secure by Default	Cisco TMS understands the ability for systems to support encryption or not, and this setting will control the default behavior for Scheduled Conferences. *If Possible* is the default and will enable encryption when all systems in a call support.

Adding and managing systems

To add, manage, and organize systems in Cisco TMS, go to **Systems > Navigator**. Systems in Cisco TMS include:

- endpoints
- gateways
- gatekeepers
- MCUs
- equipment
- rooms

The Navigator presents all systems organized in a hierarchical folder structure, similar to your computer's file system. In a new installation, two default folders are displayed in the list on the left side of the page:

- A root (top level) folder named **Company Name**.
- A child folder named **Discovered Systems**.

Default System Navigator

The page is organized into two panels with a tree view on the left side. Select an item in the tree view to see the details for that item in the right-side panel.

Adding, moving, or removing systems can only be done from the folder view. However, you can change the tree view to display systems by type, status, manufacturer, and so on by using the drop-down list at the top.

Setting up default system folders

Administrators can define any folder structure they like under the root folder. The folders are purely for organizational purposes, making it easier to locate systems and set system permissions. The same folder tree is seen by all users, and is used throughout Cisco TMS, so administrators should choose a scheme that is friendly and understandable for all user groups who need to access Cisco TMS. A common model used is one based on geography and organization, like the below example:
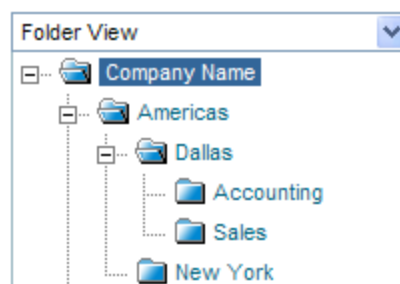
To build your own folder structure:

1. Click on the **Company Name** folder in the tree. The right panel will update to show the contents of that folder.
2. Click the **Edit this Folder** button at the top right side of the screen.
3. Rename the folder with the appropriate company name.
4. Click **Save**.
5. Add any additional folders you wish to add. To add a folder:
   a. Click on the parent folder you want from the tree.
   b. In the right panel, click **Make New Folder**.
   c. Enter a name and description (optional).
   d. Click **Save**.
   e. Repeat steps a-d for as many folders as you wish to create. You can also add and remove folders at a later time.

Adding a system

There are four different ways to add systems to Cisco TMS, represented by four different tabs in the interface:

- **Add Systems**: Add systems by IP range, comma-separated IP or host address list.
- **From List**: Add existing systems to a new folder, including systems that have been auto-discovered by Cisco TMS.
- **Pre Register Systems**: Have a system register automatically when it comes online. Enter a system name and primary identifier (MAC address recommended), and select whether to apply a configuration template.
- **Add Rooms/Equipment**: Add rooms or equipment such as projectors or dvd players. Advanced settings are available when adding rooms.

Refer to the help system for detailed information on the available settings on each tab. The following example uses the **Add Systems** tab:

1. Go to **Systems > Navigator**.
2. Open **Discovered Systems** to verify that the system you are planning to add has not been added automatically by Cisco TMS already. Automatic System Discovery is enabled as part of the installation.
   - If the system has already been added, proceed to Updating automatically discovered systems.
   - If the system is not in the **Discovered Systems** folder, select the folder you want the system added to.
3. Click **Add Systems**.

4. Enter the IP address or hostname for the system, an IP range or a comma-separated list of IP addresses and/or hostnames. Note that adding very large ranges slows down the system discovery scan process.

5. Select time zone, IP zone, and ISDN zone for the system from the drop-down lists.
6. Click the **Advanced Settings** panel bar to expand it if you need to add authentication details, configuration template, or SNMP discovery options.
7. Click the **Next** button at the bottom of the page to start adding the system. A progress window will be shown as Cisco TMS connects to the address and determines the type of system being added, and the system's configuration.
8. If a password is needed to access the endpoint, Cisco TMS will prompt you. Enter the password and click **Next**.
9. When Cisco TMS successfully adds a system, it will configure the management settings needed for the system to communicate with Cisco TMS. After Cisco TMS has contacted and interrogated the system, a **Results** page is shown with a status for each system it tried to add. If Cisco TMS detected problems with a system's configuration, a message in the **Description** column states that the system has not yet been added.

Add Result				
Systems found:				
☐ Network Address	System Name	System Type	Description	Actions
☑ 10.1.2.83	Rack MXP-12	TANDBERG MXP Endpoint	✗ Not yet added: Wrong System Settings	Edit System
Add System Despite Warnings	Remove Systems			
Finish Adding Systems	Add More Systems			

Do one of the following:

*   Click **Edit System** to edit the system's settings. A description of the error will be displayed in the settings page. Edit the settings as necessary and click **Save**. If the problem is resolved, the settings page will close and you will be returned to the **Results** page where the Description has been updated to show the system was successfully added.
*   If you want to fix the errors later or ignore the messages altogether, click **Add System Despite Warnings** on the **Settings** or **Results** page.

10. Click the **Finish Adding Systems** button to return to the **Navigator** view. Your new system will now be in the designated folder.

Refer to *Cisco TelePresence Management Suite Administrator Guide* for detail on adding specific system types, such as Cisco Unified Communications Manager, and content and recording servers.

Viewing and editing a managed system

When a system has been added to Cisco TMS, it can be managed using the web interface:

1. Go to **Systems > Navigator** and locate the system in the Navigator tree or by navigating to its folder and clicking on its name in the folder's listing in the right panel. The right panel will update to show the system's information. The default view is the **System Summary** tab. This view gives you an overview of the system and its essential numbers and status.
2. Click on the other tabs to toggle other views that give more details about the system, such as active call details, phonebook configuration of the system, connection details for the system and quick access to logs for this system.
3. Click on the **Settings** tab to show a more detailed view of the system's configuration.
    *   The **Force Refresh** button at the bottom of the page allows you to force Cisco TMS to refresh its view of the system's settings immediately if required.
    *   Click **Edit Settings** in the menu bar to edit any of the system's settings and Cisco TMS properties.
    *   Most systems can be rebooted from this screen by clicking **Boot**.

Connection parameters

If Cisco TMS is unable to communicate with the system, the **Connection** tab is displayed showing the parameters Cisco TMS uses to communicate with the system.
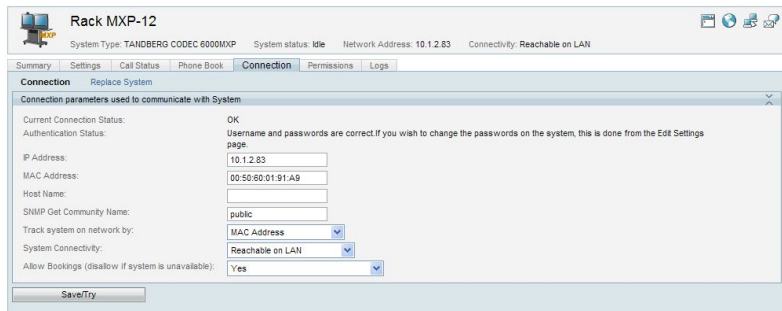
Connection Settings Tab

To attempt reconnecting with the system:

1. Update any settings as required.
2. Click **Save/Try**.

Updating automatically discovered systems

Before completing your initial configuration of Cisco TMS, review the settings of any systems that have been automatically discovered and added to Cisco TMS:

1. Go to **Systems > Navigator > Discovered Systems**.
2. View the configuration of each system and update any settings, including ISDN and IP Zones where necessary.
3. Check the Permissions tab to see whether new user groups will have permissions for the system. Modify as required.
4. If desired, move the systems to a more permanent folder by selecting the system's checkbox and clicking **Move/Copy** in the folder listing.

Cisco TMS will notify you by email whenever it discovers a new system from the **System Notification** setting you configured in a previous step. After receiving a notification, you can view the newly added system, review its settings and update it as necessary to suit your needs.

Working with phone books

A key feature of Cisco TMS is the ability to offer centralized phone books for managed systems.

We recommend during initial configuration that you familiarize yourself with how phone books are assigned to systems.

A phone book is a listing of contacts:

- Local phone books are the directories stored and available on most endpoints. These are normally set up and edited directly on the endpoint itself.
- Server phone books are phone books managed by Cisco TMS. Multiple phone books can be created in Cisco TMS and each one can be assigned to different users-groups and systems. Each contact entry can include ISDN, IP, SIP, and telephone numbers.

To create or manage phone books, go to **Phone Books > Manage Phone Books**.

Phone book sources

A phone book in Cisco TMS can be populated from one or more phone book sources. Cisco TMS can create phone books from a variety of sources including Active Directory, H.350 Servers, Gatekeepers, and files.

To create or manage phone book sources, go to **Phone Books > Manage Phone Book Sources**.

Setting phone books on a system

This is the process that associates a system with a phone book so that the system can read and display the phone book contents.

Phone books can be set on any number of systems, and each system can have multiple phone books associated with it. This allows you to create phone books for different purposes and assign them to the specific systems that need them.

To set phone books on one or more systems, go to **Phone Books > Manage Phone Books**. It is also possible to assign phone books to an individual system in System Navigator using the **Phone Book** tab when viewing a system.

Access control

Use Cisco TMS user groups to define which users get read access to the different phone books.

If provisioning is enabled, use Provisioning Directory groups to define which provisioned users shall have access to each phone book.

The default phone books

Two default phone books are created as part of the initial installation:

- A simple phone book that contains all systems managed by Cisco TMS, assigned to all the systems that Cisco TMS automatically discovered. The phone book starts with a list of all the current Cisco TMS systems, and this list comes from from a phone book source that was created during installation.
- A Provisioning Phone Book containing all users found in the Provisioning Directory if the Cisco TMS Agent is enabled. This phone book is created from the Provisioning Phone Book source. Note that if FindMe is not being used, and only the Device URI is used in the Provisioning Directory, then the Provisioning Phone Book Source will not be populated until users begin to log into their devices.

Creating a scheduled conference

When scheduling conferences with Cisco TMS, it is not necessary for the user to worry about network protocols, MCUs, or gateways. Cisco TMS handles infrastructure choices and compatibility checking of all these things automatically. Advanced users may still tune and tweak the selected methods for the conference as needed.

Several interfaces for scheduling conferences are available depending on the need of the user:

- Scheduler is an interface aimed at a general audience, with administrator-defined limits on the allowed settings.
- **Free/Busy Overview** is best when you just need to know which systems are available for a quick meeting.
- **New Conference** is the most robust interface, as it offers all the possible control and settings available in Cisco TMS. This page is used in the procedure described below.

To book a conference:

1. Go to **Booking > New Conference**.

New Conference

2. Enter a conference title. It will be displayed in all Cisco TMS interfaces, and in email notifications about the conference
3. Set the start time and the duration or end time for the conference.
4. Click **Recurrence Settings** to create a series of meetings that are tied together, such as a weekly or daily meeting.
5. In the **Advanced Settings** section, set configuration options for this conference. Most settings will take their default values from the Conference Default values configured under **Administrative Tools**. Refer to the help for an overview of all available settings. Note that if **Secure** is set to *Yes*, Cisco TMS will only allow systems that support encryption to participate in the conference.
6. Optionally, add notes about the conference in **Conference Information**.

7. In the **Participant** tab, click **Add Participant** and a new window will appear.
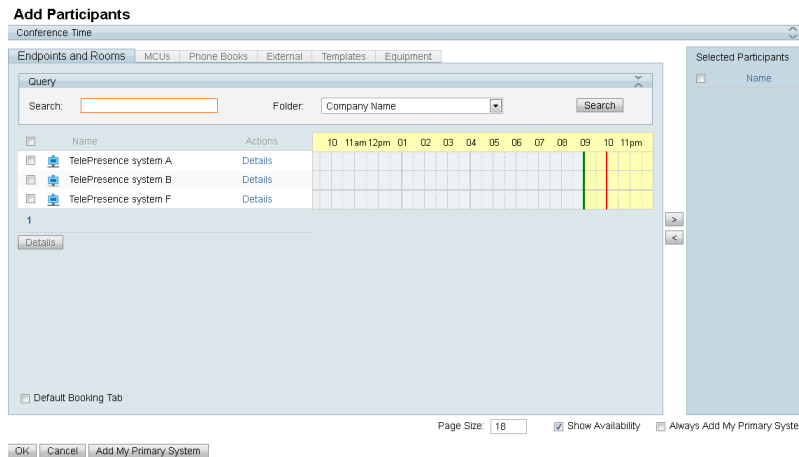
Add Participants

- Available participants and a planner view with their availability is displayed based on existing scheduled and ad hoc meetings. The colored vertical lines represent your current requested time for the scheduled meeting.
- Click the tabs to have participants listed by type. If you have used scheduling before, the default tab is **Last Used** with quick access to the systems you have used recently.
- Hover any system, or the blocks in the planner view, for additional detail about the system or scheduled meeting.

8. Add participants to the meeting by selecting their checkbox and clicking the **>** button to add them to the list of selected participants on the rights side of the window. Adding network infrastructure components like MCUs and Gateways is optional as Cisco TMS will handle this for you automatically.

9. Use the **External** tab to add systems not managed by Cisco TMS, for example systems in other organizations, or telephone participants.
    - For dial-out participants, enter their contact information, and Cisco TMS will automatically connect them to the conference at the scheduled time.
    - For dial-in participants, Cisco TMS will reserve the capacity needed to host the site in the conference and will provide you with precise dial-in information to forward to the participant.

10. Click **OK** when all participants have been added.

11. You will be returned to the conference page, with the participant section of the page now showing your selected participants, and some additional tabs. These additional tabs allow advanced scheduling tasks such as altering how calls are connected, or setting specific MCU conference settings for the conference.

12. Use the **Video Conference Master** drop-down list to determine which system should be considered the meeting organizer. Not all telepresence systems support the necessary features for this functionality, and only systems that are eligible will be displayed in this list. This is the system that will be prompted:
    - to connect the conference if it is not scheduled for automated call launch.
    - to extend the conference when it is about to expire.

13. Click **Save Conference**. When the conference is saved, Cisco TMS will do all the routing calculations to determine the best way to connect your selected participants.
    - If Cisco TMS is able to complete your request:
        i. You will be presented with a **Confirmation** page showing the details of your meeting, including the participant list and listing how each of those participants are scheduled to connect to the conference and the exact dial string any participants must dial.
        ii. You will also receive an email confirmation with an ICS attachment for saving the event in your Outlook (or compatible) calendar.

- If Cisco TMS is unable to complete your booking request:
  i. You will be returned to the **New Conference** page. A message banner states why it was not possible to save the meeting. This may be due to lack of availability, lack of network resources, or there was no known route to connect the participants together.
 ii. Edit the conference settings to try to resolve the issue and try saving the conference again.

Viewing and editing existing conferences

To see details about an upcoming or completed conference, use the **List Conferences** feature. You will be able to see:

- all the settings that were configured for the conference
- the route that Cisco TMS built to connect the conference
- a log of events for the conference.

If the conference is scheduled for a time in the future, you can also modify the conference settings from this view.

1. Open **Booking > List Conferences**
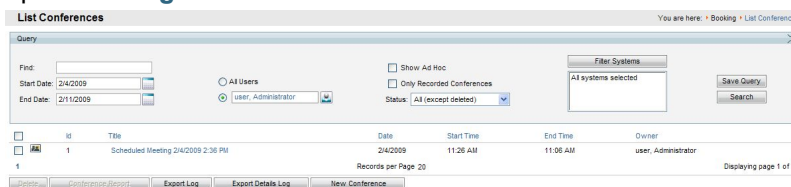
List Conferences Page

The default view is a list of conferences owned by you. If you wish to see all conferences, select **All Users** and click **Search**.

2. To view a conference, find it in the list below and hover over the title. Open the drop-down menu and select **View**.
3. The resulting page looks like the **New Conference** page.
   - Click on the tabs in the lower segment of the window to see the information saved for this conference.
   - If the conference is scheduled for the future, you can click the **Edit** button to modify the meeting using the same options as when creating a new conference. The conference will be updated and new confirmation email messages will be distributed.

Monitoring and managing ongoing conferences

You can monitor and control scheduled and ad hoc conferences in real-time. The most advanced views and controls are available from the **Monitoring** menu in Cisco TMS. This menu has three interactive real-time applications to work with, described below.

Conference Control Center

The **Conference Control Center** (CCC) is a dashboard-like interface that allows you to monitor the status of the conferences running on the network and additionally dive in and actually control and interact with the systems in the conference.

From this control center you can create operator conferences; ad hoc conferences that let conference operators work with individual participants in a conference outside their normally scheduled call.

This means that if a site is having a problem, or has questions, an operator can start a new conference and add themselves and the problem site(s) to the special conference. When this conference is done, the operator can send the site back to their originally scheduled call.

For detail on creating operator conferences, refer to the built-in help system.

Graphical Monitor

The **Graphical Monitor** is an interactive live "map" of your conferencing network. Using animation and colors, it shows a live view of your network including active calls, and systems that are unreachable. The view is based on the folder structure set up in the System Navigator.
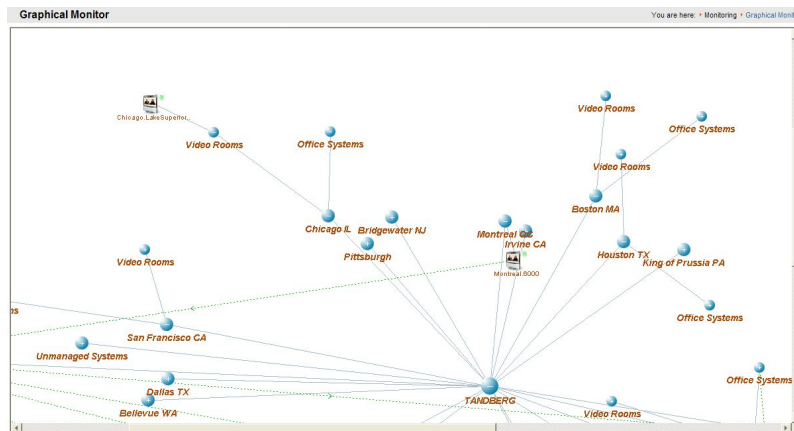
Graphical Map Monitor

The **Map Monitor** is a variant of the Graphical Monitor where instead of all systems being shown on one page, each folder has its own page and administrators may overlay graphics behind the icons and

images. This is very useful for showing geography or system location information.

Reporting

Cisco TMS constantly collects data from the systems that it manages, as well as logging activity that takes place in Cisco TMS itself. The Reporting section gives administrators the ability to visualize and review historical data from their conferencing network.

Cisco TMS collects valuable data such as:

- Call Detail Reports
- Diagnostic Events and Alerts from systems
- Details on how people are scheduling calls
- Comparisons of scheduled versus actual usage
- An ROI Calculator based on actual conferencing usage

The different categories of reports are available from the **Reporting** menu, and all reports use the same basic interface.
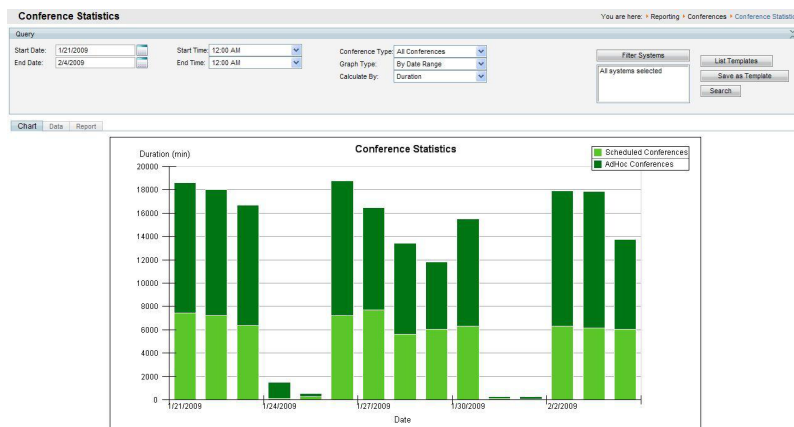
Example report from the Conferencing Statistics Report.

Each of the reports shares the following tools:

- Filtering - The top section provides filter and search criteria to allow you to control what data the report encompasses, including date ranges, types, and systems or users to include. You can also save a group of settings as a Template to reuse later by clicking **Save as Template**.
- Chart View – A graphical representation of the data. The chart type depends on the data being displayed, including line, bar or pie charts.
- Data view - The actual data in the report, such as the call history, event log, or conference history, shown in a table format. This information can be exported to Excel for further analysis by clicking **Export to Excel**.
- Report View - Puts the Chart view into a presentation format that can be exported to a PDF file by clicking **Export to PDF**.

See the Cisco TMS Administrator Guide and Online help for further instructions.

Appendices

In this section:

- Appendix 1. Restricting IIS 7 modules to minimal required describes an optional security measure.
- Appendix 2. Uninstalling Cisco TMS details how to uninstall the application and remove all components from the server.

Appendix 1. Restricting IIS 7 modules to minimal required

IIS 7 offers a modular system that allows an administrator to fine tune what components are installed and enabled on their server for the greatest security. To assist administrators who wish to further restrict their servers, the following list documents which modules are required for Cisco TMS. Modules may be controlled at either the site or server level (some are server level only) . The steps below assume that you are making changes at the server level.

Before removing modules, we recommend backing up your IIS configuration by using the command `%windir%\system32\inetsrv\appcmd.exe add backup "TMS"`.

To restore the backup later if needed, use the command `%windir%\system32\inetsrv\appcmd.exe restore backup "TMS"`

To modify which modules are enabled in IIS 7:

1. Open the **Internet Information Services (IIS) Manager** from **Start Menu > Administrative Tools > Internet Information Services (IIS) Manager**.
2. From the Tree in the left panel, click on your server's name.
3. In the center panel, under **IIS**, double-click **Modules**.

The list of installed Managed and Native Modules is displayed. Modules that are not needed can be removed by clicking on them, and then clicking **Remove** from the Action Panel on the right.

The following modules are required for Cisco TMS and must *not* be removed:

- **AnonymousAuthenticationModule**
- **BasicaAuthenticationModule**
- **DefaultDocumentModule**
- **DefaultAuthentication**
- **DigestAuthenticationModule**
- **HttpCacheModule**
- **HttpLoggingModule (recommended)**
- **HttprRedirectionModule**
- **IsapiFilterModule**
- **ProtocolSupportModule**
- **RequestFilteringModule**
- **Session**
- **StaticCompressionModule**
- **StaticFileModule**
- **WindowsAuthentication**
- **WindowsAuthenticationModule**

Appendix 2. Uninstalling Cisco TMS

This section tells you how to remove the Cisco TMS application: this is not necessary under normal conditions because older versions of Cisco TMS are removed automatically by the Cisco TMS installer. This information is provided for reference and for advanced troubleshooting.

Caution: If you are doing replication between Cisco TMS and Cisco VCS, disable the replication before beginning the uninstall.

Uninstalling Cisco TMS removes the Cisco TMS application, web site, and services. It leaves customer data, logs, databases and database servers intact for use in future upgrades. The uninstall wizard does not modify the SQL server or the OpenDS server in any way see the next section if you want to completely remove all Cisco TMS information from the server, including the database servers.

To remove the Cisco TMS application:

1. Select '*Uninstall Cisco TMS*' from the Cisco program group in the Start Menu or use Add/Remove Programs in the Windows Control Panel.
2. A welcome window explains that the uninstallation script removes Cisco TMS, but the database and database server must be removed separately. Click **Next**. The wizard removes the Cisco TMS services, website, and application data.
3. When prompted to restart your computer, select *Restart now* and click **Finish**.

Removal of the Cisco TMS application is complete.

Removing all Cisco TMS information from a server

The uninstall wizard only removes the Cisco TMS application from the server so that Cisco TMS can easily be reinstalled or upgraded in the future.

CAUTION:

- These steps assume that the SQL server was installed by Cisco TMS, is not being used by any other applications, and is safe to remove. Do not remove the SQL server or its program folder if the SQL server is used by any other application.
- Following these steps will delete *all* Cisco TMS data. Do not proceed if you intend to save any information from your Cisco TMS installation.

To completely remove Cisco TMS and all of its data from your server, follow these instructions:

1. Run the Cisco TMS uninstall wizard using the instructions in the previous section.
2. Navigate to the Provisioning\OpenDS folder of the Cisco TMS installation, by default C:\Program Files\TANDBERG\TMS\Provisioning\OpenDS.
3. Double-click "uninstall.bat" to start the uninstall wizard for the Cisco TMS Agent database. A selection screen is displayed.
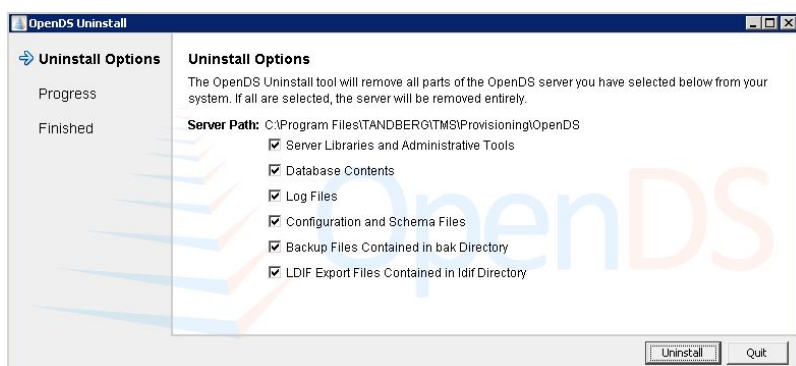
4. Ensure that all options are selected, and click **Uninstall**.
5. At the warning stating that the server is currently running, click **Yes** to have the wizard stop the service for you.
6. When the database and its files are successfully uninstalled, click **Close**.
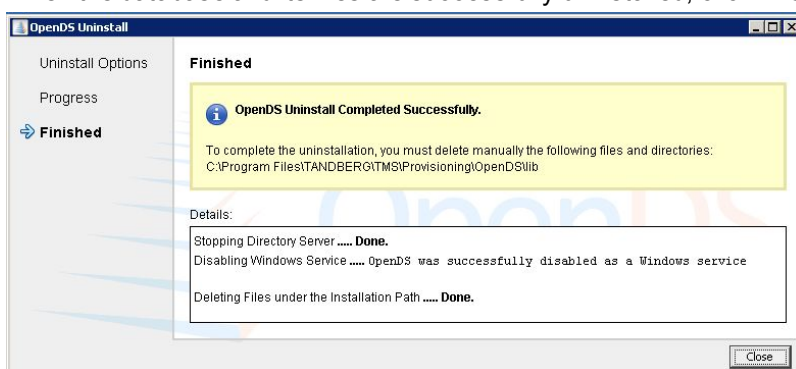
7. Delete the program folder used by the Cisco TMS installation. The default location is **C:\Program Files\TANDBERG\TMS**.
8. Open the Windows registry editor: from the Start menu, select 'Run..' and enter 'regedit' and click **OK**.
9. Expand the tree on the left using the plus icons to find the Hive (folder) **HKEY_LOCAL_ MACHINE\SOFTWARE\Tandberg\TANDBERG Management Suite**.

10. Right-click on the Cisco Management Suite folder icon, and click **Delete**. Click **Yes** to confirm.
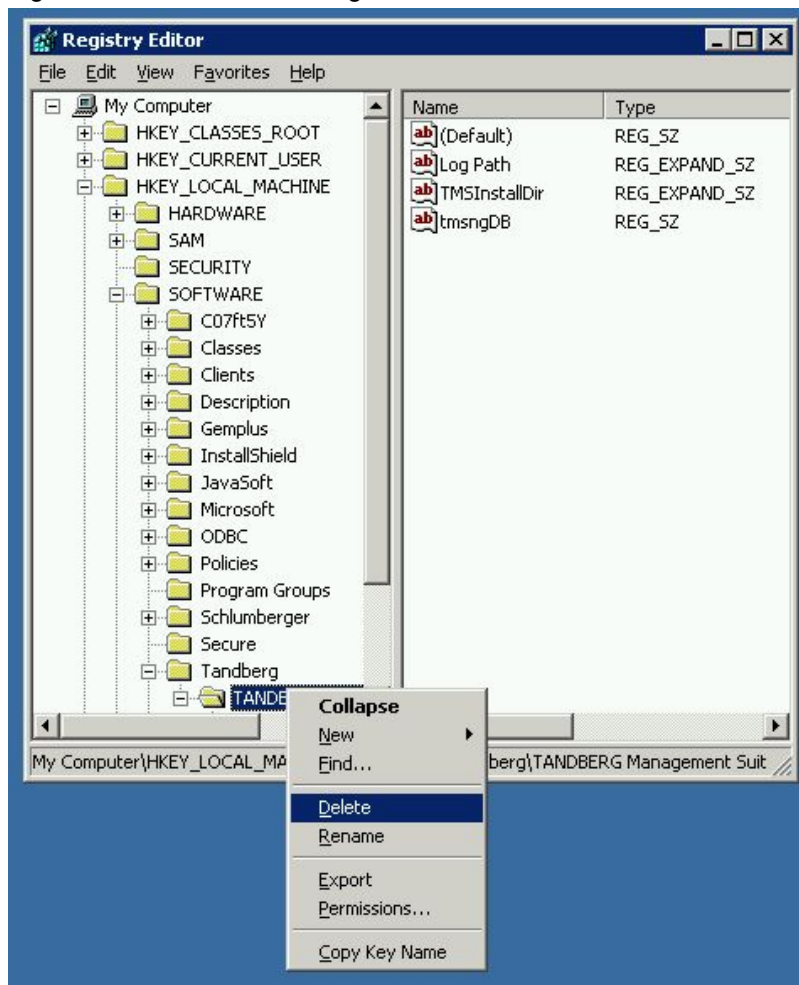
Deleting the Cisco TMS Registry Key

11. Close the Registry Editor.
12. If you were using a remote SQL Server, ask your SQL Administrator to drop the database named **tmsng**.
13. If the Cisco TMS installer installed a local copy of SQL Server, complete the following steps to remove it:
    a. Open **Add/Remove Programs** from the Windows Control Panel.
    b. Find "Microsoft SQL Server" with the relevant version number (2005 or 2008 depending on your installation) in the list and click **Remove**.
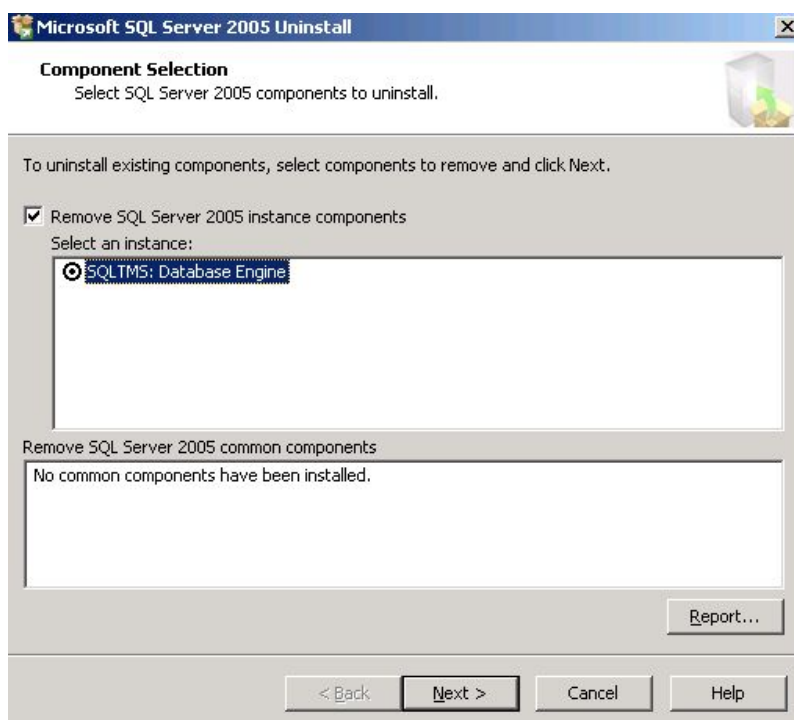
c. Check **Remove SQL Server 2005 instance components**.
d. Select **SQLTMS: Database Engine**.
e. Select **Workstation Component** from common components.
 f. Click **Next**.
g. At the Summary page, click **Finish**. The wizard closes automatically when complete.
h. Delete the program folder used by the SQL installation. The default location is C:\Program Files\Microsoft SQL Server.

The removal of Cisco TMS, the database servers, and all customer saved data is now complete.

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
Cisco TelePresence Management Suite Release Notes (13.1)	D14837
Installing licenses; release and options keys for the Cisco TelePresence Management Suite	78-19878-01
Cisco TelePresence Management Suite Administrator Guide (13.1)	D13741
Cisco TelePresence Management Suite Provisioning Deployment Guide	D14368
Cisco TelePresence VCS Deployment Guide - Cluster creation and maintenance	D14367
Cisco TelePresence VCS Software Release Notes (X5)	D50582
Cisco TelePresence Management Suite Release Notes (v12)	D50539
Cisco TelePresence Management Suite Product Support (12.2)	D50546
Cisco TelePresence Management Suite Release Document (v11)	D50418
Cisco TelePresence Implementing Secure Management Configuration Guide (13.0)	D50520
Cisco TelePresence Management Suite Database Knowledge Tips	D14216