Cisco TelePresence Management Suite

Installation and Getting Started guide

D14389.04

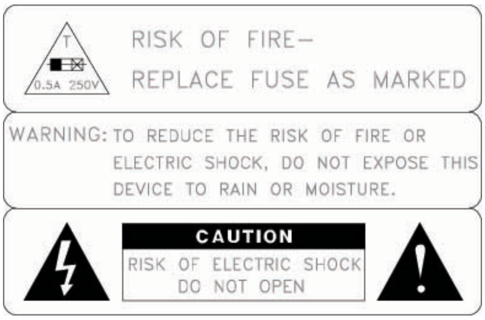
January 2011

Operator safety summary (appliance)

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 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.


T
0.5A 250V
RISK OF FIRE–
REPLACE FUSE AS MARKED
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 the equipment 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 the apparatus from the 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 the installation 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 the power cord so as 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 – It is recommended systems 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 the cart/apparatus combination to avoid injury from tip-over.
- Lightning - Unplug this 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 the apparatus from the outlet and refer servicing to qualified personnel under the following conditions:
  - When the power cord or plug is damaged or frayed
  - If liquid has been spilled or objects have fallen into the apparatus
  - If the apparatus has been exposed to rain or moisture
  - If the apparatus has been subjected to excessive shock by being dropped, or the cabinet has been damaged
  - If the apparatus fails to operate in accordance with the operating instructions

Table of Contents

Introduction

The Cisco TelePresence Management Suite (Cisco TMS) is a portal for managing and monitoring your video conferencing system 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 can be downloaded from Cisco.com.

Cisco TMS is a powerful tool for maintaining, operating, and increasing the value of your conferencing network. Cisco TMS adds intelligence, diagnostics, and functionality that enhance your video network components and the return on your investment.

Cisco TMS automates system configuration for a basic H.323 network, operating ‘right out of the box’. You can tune Cisco TMS default behavior to suit your organization 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 installs, upgrading an existing version, or configuring the Cisco TMS version that comes preinstalled on a Cisco TelePresence Management Server. There is also a guide for uninstalling Cisco TMS.

Along with installation/upgrade processes, you will find guidelines on software and hardware requirements, integrating Cisco TMS with other applications, and version specific upgrade information.

Further information on Cisco TMS functionality is available online. Cisco also maintains a Cisco TMS knowledgebase.

Note: For the Cisco TMS user guide, see the online help available via the question mark icon (?) on the Cisco TMS client.

A list of relevant documents referred to in this guide can be found in the References and related documents section.

Cisco TMS requirements

This section details software and hardware requirements. Review and verify these requirements before installing, upgrading or configuring your preinstalled Cisco TelePresence Management Servers.

Operating system

Previous versions of Cisco TMS required a 32bit Windows operating system.

Note: As of version 13 Cisco TMS functions with 64bit Windows 2008 operating systems. See below for further details.

The operating system must be English, Japanese or Chinese.

Web server

Hardware Specifications

Pentium compatible processor:	2GHz or higher
Memory:	1GB RAM or more (2GB or more recommended) For Provisioning, 2GB or more is recommended. The installer will warn you during installation if less than 2GB is detected.
Disk Space:	4GB for installation and application footprint (Additional space is required if you are installing the SQL Server locally)

Version compatibility

The following Windows versions are compatible with Cisco TMS:

- Windows 2003 Server Standard/Enterprise/DataCenter Editions w/SP1 or greater (latest Service Pack recommended)
- Windows 2003 R2 Standard/Enterprise/DataCenter Editions w/SP1 or greater (latest Service Pack recommended)
- Windows 2008 R1 or R2 Standard 32bit and 64bit Editions (latest Service Pack recommended)

Windows Server 2000 is no longer supported

Microsoft Windows Server 2000 (any version) is no longer supported. Customers running Cisco TMS on a Windows Server 2000 OS must upgrade their server to Windows Server 2003. See Upgrading Windows 2000 to Windows 2003.

Microsoft .NET Framework 4.x now required

Cisco TMS 13.x requires Microsoft .NET Framework version 4.x. The Cisco TMS installer prompts you to install .NET 4.x if it is not detected. (Previously, Cisco TMS 12.x required Microsoft .NET Framework version 3.5).

IIS 7 is required

If you are using Windows 2008 Standard 32bit or 64bit Editions, the installer will install IIS 7 if it is not already present.

Windows 2008 default firewall rules

Windows Server 2008 includes a new Windows Firewall feature that controls both inbound and outbound ports. This feature is enabled by default. If Windows Firewall is enabled, the ports required for Cisco TMS must be opened. For details see Ports required by Cisco TMS.

SQL database server

SQL Server version compatibility

Note: Microsoft SQL Server 2000 Desktop Engine (MSDE 2000) and Microsoft SQL 2000 are no longer supported. Assistance on upgrading to SQL 2005 Server can be found in the Cisco TMS Database Knowledge Base Tips.

Cisco TMS supports:

- Microsoft SQL Server 2005 Database Server with Mixed Authentication Mode enabled. All 32bit versions of Microsoft SQL Server 2005, including the Express Edition (see caveat below).
- Microsoft SQL Server 2008 both 32bit and 64bit.
- If you are installing SQL Server 2008 on the same server as Cisco TMS, .NET 2.0 SP2 is required.

Note: Large installations with databases more than 4GB must use a full edition of SQL Server 2005, because of the 4GB database limitation in Express Edition.

If there is not an SQL DB present on the server, MS SQL Server 2008 Express 32 bit will be installed.

Cisco TMS operational

The following are required by Cisco TMS to function properly:

- **Domain Membership Preferred** – Each user logging into Cisco TMS needs a Windows User Login to authenticate: 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, trusted domain users will automatically be able to use their Windows credentials to log into Cisco TMS. You can still limit user permissions using Cisco TMS. Active Directory membership is the recommended deployment for most installations because it avoids creating local Windows accounts for each user.
- **ASP.NET and ASP Enabled** – These IIS components must be enabled. If you are using Windows 2008, see Installing IIS 7 for Windows 2008.
- **Cisco TMS Web site Accessible by IP and Hostname** - Because not all devices support DNS hostnames or Port Numbers, Cisco TMS must be accessible by an IP Address on port 80. Some functionality requires Cisco TMS to be reachable by hostname; therefore, Cisco TMS is also accessible by a fully qualified hostname.
- **Mail Server Access** - Cisco TMS requires access to an SMTP (Mail) server to send emails. Cisco TMS does not require its own SMTP server and can be configured to use existing mail servers. If you are unsure which server to use, contact your IT administrator. (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. The specific protocols and directions in use will vary depending on devices being managed: see the Cisco TMS Product Support document (available on the Cisco TMS installation media) for specific information about firewall requirements for each type of supported device.
- **DNS records and Provisioning Directory functionality (Cisco TMS Agent)** – In installations using the Cisco TMS Provisioning Directory functionality for Cisco TelePresence Movi and E20

deployments, the local hostname of the Cisco TMS server **must** match the DNS A record for the Cisco TMS Agent to operate correctly.

- **TCP Port 25** – Many anti-virus programs block applications from sending mail directly using the SMTP Port (TCP Port 25). Verify your anti-virus program is configured to allow this.

Cisco TMS client

Cisco TMS is accessed by both administrators and users via a web browser. Disable all pop-up blocking functions for the Cisco TMS web site.

Minimum specifications

- Microsoft Internet Explorer 6.0 or later
- Mozilla Firefox 2.0 or later
- Java Virtual Machine Runtime Engine (JRE) 1.5.0 or later
- A Windows username and password to the Cisco TMS Server (either a local machine account, or a domain account, if the server is joined to a domain)

Recommended specifications

- Microsoft Internet Explorer 7.0 or 8.0
- Mozilla Firefox 4.0 or 5.0
- Java Virtual Machine Runtime Engine (JRE) 1.5.0 or later

A Java Virtual Machine Runtime Engine (JRE) is required to use the Cisco TMS monitoring function. If browser does not automatically prompt to download and install the missing browser plug-in, you can install it manually from the JRE installation file found on the Cisco TMS installation media or at http://www.java.com.

Installation and upgrade guidelines

Cisco TelePresence recommend reviewing these guidelines before installation or upgrading, and cover a number of issues that may relate to your Cisco TMS application.

Moving the Cisco TMS database

To move the Cisco TMS database to a new server, it is recommended the database and/or database server be moved prior to running the Cisco TMS v12 installer. Use the standard Microsoft SQL tools (the Cisco TMS database is named 'TMSng'), and then select 'Custom' during the Cisco TMS v12 installation. You can then specify the database location.

Dedicated vs. shared server

Cisco TMS is resource intensive with specific server requirements and installation is not recommended on a server hosting other applications or web sites. CPU time and memory usage will vary between installations depending on the activity level and size of the video network being managed.

Note: Cisco TelePresence will not support installations on shared servers. Cisco TelePresence strongly recommends installing Cisco TMS on a dedicated server.

Cisco TMS can be installed on a Virtual Server, but the Cisco TMS virtual machine (child partition) must be provided with sufficient processor resources, memory, and disk resources. The minimum requirements assume Cisco TMS has full access to resources. Cisco TMS runs on VMWare ESX and Virtual Server products and on Microsoft Virtual Server 2007.

Cisco TMS integration compatibility matrix

Note: The most recent software versions may be required for all features and fixes to be available.

Product	**Compatible Version**
TANDBERG See&Share	v3.3
Cisco TelePresence Microsoft Exchange Integration	All Versions
Cisco TelePresence Microsoft LCS Integration	All Versions
Cisco TelePresence Conferencing eXtensions	All Versions
Cisco TMS – IBM Lotus Notes Integration	All Versions
Cisco TMS - IBM Lotus Sametime Integration	All Versions
Cisco TelePresence Movi for IBM Lotus Sametime	All Versions
Cisco TelePresence Management Suite Extension Booking API	All Versions

Device support

Cisco TMS supports video conferencing systems from both Cisco TelePresence and other major vendors, and Cisco TelePresence constantly strives for the best possible feature parity. However, due to differences in capabilities and APIs, some features of Cisco TMS and device support are dependent on the individual products and their software versions. Some system types require additional configuration.

Cisco TelePresence maintains Cisco TMS Product Support Documentation, including information on:

- version compatibility information
- network requirements (firewall information)
- device configuration settings

- feature support
- device notes

This information is available on the Cisco TMS installation media and the Cisco TelePresence support web pages. Be sure to use the revision of the document that applies to your Cisco TMS version.

SQL database server guidelines

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.

Disk space

Smaller deployments (<100 systems) can, on average, expect database sizes on the order of 50MB – 2GB. Medium deployments (100-500 systems) can expect databases on the order of 1GB-6GB, and very large or very heavy networks can expect databases of approximately 6GB-10GB.

Microsoft SQL Server automatically sets and manages database size. Cisco TMS also provides a method to manage growth in **Administrative Tools > TMS Server Maintenance**, where you can set data retention limits.

Local vs. Remote server

The SQL database server and Cisco TMS can be both be hosted on the same machine, or on separate machines. During installation, you can choose between using an existing SQL Server or installing MS SQL Server 2008 Express 32 bit locally on the Cisco TMS server.

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. A separate server solution improves Cisco TMS performance by freeing up memory and disk resources.

If your TMSng database is on an external Microsoft SQL Server 2005, set the Microsoft SQL Server compatibility level 90.

Database permissions

The SQL database server must have Mixed Mode Authentication enabled; Windows Authentication is not supported by the Cisco TMS installer. For new installations, the installer creates a database named ‘TMSng’ using the SQL Server defaults. Upgrades will reuse an existing Cisco TMS database.

When installing or upgrading Cisco TMS and using an existing SQL Server, the Cisco TMS 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 a 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 and assign itself as the owner. Cisco TMS will 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 SQL_Latin1_General_Cp1_CI_AS or SQL_Latin1_General_Cp1_CS_AS.
  - An SQL user and login to use for the Cisco TMS Service account and grant the user the ‘dbowner’ role for the ‘TMSng’ database.

When you are prompted for the SQL Server credentials during installation, enter the username and password for that account. The Cisco TMS installer will populate the ‘TMSng’ database as required, and will continue to use this account to access the database after installation.

Note: For Cisco TMS to function properly the SQL user supplied for Cisco TMS to use 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 Cisco TMS SQL database named 'TMSng'.

Backups can be performed on the server via a local console or Windows Remote Desktop. Additional help on performing SQL backups is available in the Cisco TMS Database Knowledge Base Tips document available on the Cisco TMS installation media. It is recommended that backups are stored at a separate location for maximum protection.

Note: The 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.

Note: A Cisco TMS Agent database backup can be performed and scheduled by going to the TMS Agent Settings page found under **Administrative Tools > Configuration > TMS Agent Settings**.

Upgrading Windows 2000 to Windows 2003

If you are upgrading from Windows 2000 to Windows 2003, Microsoft recommends performing a clean installation.

Cisco TelePresence recommends 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 Cisco TMS database backup. Then upgrade to Cisco TMS v12 or newer. Additional assistance on backing up and restoring Cisco TMS can be found in the Cisco TMS Database Knowledge Base.

Restricting IIS 7 modules (optional)

IIS 7 has a modular system that allows administrators to install and enable components to customize server security. The following modules are required for Cisco TMS. Modules may be controlled at either site or server level (some are server level only) – the following steps assume that you are making changes at the server level.

To modify which modules are enabled in IIS 7:

1. Go to **Start Menu > Administrative Tools > Internet Information Services (IIS) Manager** and open the **Internet Information Services (IIS) Manager**.
2. From the tree in the left panel, click on your server 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
   - DigestAuthenticationModule
   - HttpCacheModule
   - HttpLoggingModule(recommended)
   - HttprRedirectionModule
   - IsapiFilterModule
   - ProtocolSupportModule
   - RequestFilteringModule
   - Session
   - StaticCompressionModule
   - StaticFileModule
   - WindowsAuthentication
   - WindowsAuthenticationModule

Ports required by Cisco TMS

The default Windows Server 2008 firewall rules interfere with Cisco TMS communications. Cisco TMS will not function properly until these Windows Firewall port settings are modified.

The following ports are used by Cisco TMS and must be enabled in the Windows Firewall. See the Cisco TMS Product Support document for port specifics for each managed device type.

Administrators can disable Windows Firewall or open the ports required for Cisco TMS. See http://technet.Microsoft.com/en-us/library/cc748991.aspx for Microsoft documentation on configuring firewall rules.

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 connection is further upstream from Cisco TMS, rather than being directly connected to Cisco TMS (using multiple network interface cards).

Version specific upgrade notes

Review the notes for your current version of Cisco TMS before starting your upgrade.

Notes for upgrades from Cisco TMS 12.5/12.6

When installing and upgrading to Cisco TMS 13.0, and if the TMS Agent is being utilized or intended to be utilized, Cisco recommends that you upgrade the VCS to X5.2 or later.

Also note the .NET requirements have changed. Cisco TMS version 12.x required .NET 3.5. Version 13.x requires .NET 4.0. The installer will warn you to install the correct version of :NET if it is not detected.

With regard to DNS records and Provisioning Directory functionality (Cisco TMS Agent), DNS reverse lookups (PTR records) that were required in Cisco TMS 12.5, are no longer required for Cisco TMS 12.6/13.x. (Note that the same requirement applies to the Cisco VCS. See the Cisco VCS Software Release Notes (X5) at Cisco TelePresence support documentation.)

Within Cisco TMS 12.6, under **Administrative Tools > General Settings,** note that **Enable TMS Agents** is set to *No* by default. If enabled, Cisco TelePresence recommends going to Cisco TMS Agent Diagnostics under **Administrator Tools > TMS Agent Diagnostics** to confirm that the Local Cisco TMS Agent shows no errors and that all diagnostic tests are OK.

If any errors are found on the Local Cisco TMS Agent, then these errors need to be fixed before proceeding with replication to any Cisco VCS. Refer to the Diagnostic section within Cisco TMS Provisioning Deployment Guide for help troubleshooting errors found on the Local Cisco TMS Agent.

Warning: Upgrades will be blocked if the procedures found in this document are not followed appropriately. The error message will state that Provisioning on all clusters must be disabled before upgrading to 13.x.

Notes for all versions earlier than Cisco TMS 12.2

A onetime database clean-up is required when upgrading versions Cisco TMS 12.1 or earlier.

For a large installation this 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 count. For most installations however, this process only takes an additional minute or two.

During this clean-up process, you will see a ‘Upgrading from Cisco TMS 12.x to Cisco TMS 12.x’ notification. The progress bar may not move but the installation is still running. **Please be patient!** Do not stop or attempt to stop the installation process during this step.

For more details about this update, see the Installation and Upgrades section of the Cisco TMS 12.6 part of the Cisco TMS v12 Release Notes.

Notes for upgrades from Cisco TMS 12.1 or 12.2

If you are upgrading Cisco TMS from either 12.1 or 12.2 and Cisco VCS to X5 software, you must follow the upgrade procedures found in the Cisco VCS Deployment Guide - Cluster creation and maintenance (X5) documentation available at Cisco TelePresence online support.

Note: Your upgrade process will be blocked and need to be restarted if the procedures found in this document are not followed. The error message states that provisioning on all clusters needs to be disabled.

Notes for upgrades from Cisco TMS 12.0

It is recommended you review the Provisioning Directory Deployment Guide if:

- You have Cisco VCS clusters defined in Cisco TMS 12.0. See the section on clustering for instructions on changes to cluster configuration with Cisco VCS X4.1 software.
- You use Provisioning Directory and Movi, review software dependencies between Cisco TMS and Cisco VCS.

If you participated in the Movi Beta, it is recommended you refer to their Beta Community Point of Contact for specific upgrade instructions.

Notes for upgrades from Cisco TMS v11.x

If you are using a Cisco TelePresence Content Server (TCS) with Cisco TMS, all TCS must be running version S2.0 or later. If you are upgrading from versions prior to S2, update all the server configurations and update any future bookings (see the Supplement Notes for Manuals section of the Cisco TMS v11.6 release in the Cisco TMS v11 Release Notes document available from the Cisco TelePresence web site.

Starting with Cisco TMS v12.0, permissions underwent slight reorganization. It is recommended that administrators who implement different user levels through permissions review their user group permissions after upgrading to Cisco TMS v12, and adjust the permissions to their intended settings if necessary.

Additional Notes for upgrades from versions 9.x and 10.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. Be sure to work through the Administrative Tools settings after installation to populate and update the Cisco TMS installation. In particular, the permissions model has been overhauled and Group Permissions and System Permissions must be reviewed and updated. 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.

Additional notes for upgrade from versions prior to 9.x

Cisco TelePresence recommends a new installation rather than performing upgrade installations older than Cisco TMS 9.0., although the Cisco TMS installer will still import existing data. Server requirements have changed significantly, as well as the configuration and functionality throughout the product making most direct upgrades significantly more complex than simply performing a new installation on a new host server.

Installation and upgrade of Cisco TMS

Installation and upgrade requirements

Before you start make sure that you have:

- reviewed the Cisco TMS requirements and Installation and upgrade guidelines sections
- the Windows CD-ROM available (it may be required for installing some Windows components)
- ensured the DNS servers used by Cisco TMS contain forward lookups for the TMS server

Cisco TMS requires specific server and network elements for correct installation:

- **Administrator access to the Windows server and database. Y**ou must have administrator rights to the Windows Server. 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 permissions).
- MS DOS or access to execute *.cmd and *.bat files (not necessarily the command prompt) must be available on the server to install the OpenDS and Provisioning components.

Software requirements

These software applications are required and automatically installed if not present:

- Windows SNMP Services
- MS SQL Server 2008 Express 32 bit (an existing supported SQL Server can also be used)

If you are running Windows 2008 Standard/Enterprise/DataCenter, the following software component is required:

- IIS 7

If this component if it is not present, it is installed via the Cisco TMS installer.

Installing and upgrading Cisco TMS

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

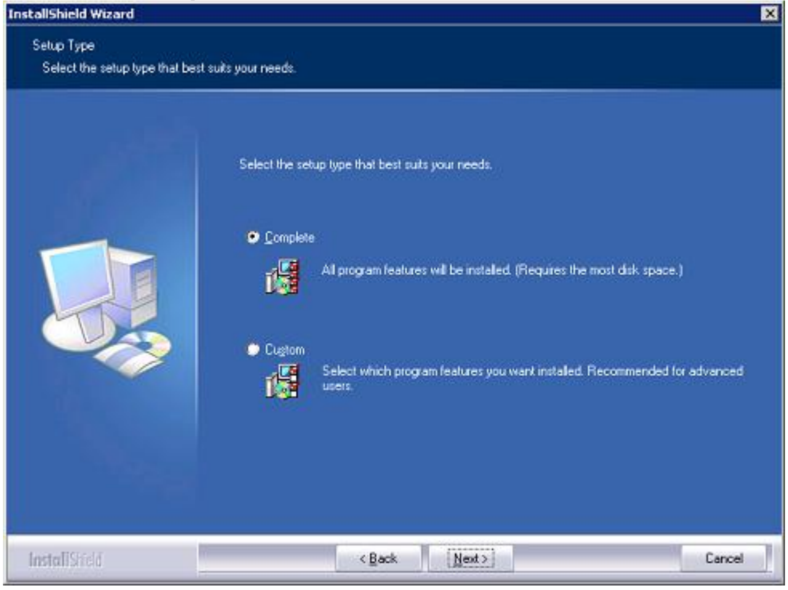
Note: You may be prompted to reboot the server more than once during installation. The installer automatically resumes after the server reboots.

Initial installation process

1. Close all open applications and disable virus-scanning software.
2. Extract the compressed Cisco TMS ZIP file to a folder.
3. Double-click **Cisco TMS executable**.
4. You will receive a language prompt. This language is only used during the installation and does not affect Cisco TMS after installation. Select the Cisco TMS Installer language and click **Next**. The installer checks for required software components. A warning message will be displayed if any components are missing. Follow the prompts and install any missing components.
5. If an earlier version of Cisco TMS is currently installed, you are prompted to upgrade. To upgrade - remove the old Cisco TMS and upgrade the existing Cisco TMS database, click **Yes**. To abort the installation and leave the current installation untouched, click **No**.
6. You are prompted to choose from two processes: Complete or Custom. They are detailed in the following two sections.

- Complete uses 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.
- Custom allows you to specify all the options such as the installation path and SQL server choices.

7. Select **Complete** or **Custom** and click **Next**.



InstallShield Wizard

Setup Type

Select the setup type that best suits your needs.

Select the setup type that best suits your needs.

● Complete

All program features will be installed. (Requires the most disk space.)

○ Custom

Select which program features you want installed. Recommended for advanced users.

Figure 1 Select Complete or Custom.

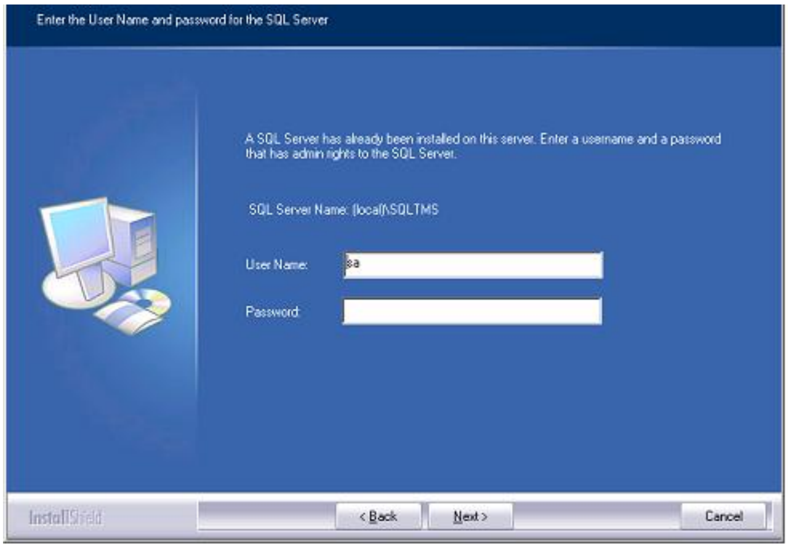
Complete installation process

Follow the process in this section if you chose ‘Complete’ for your installation type.

8. The installer searches for an existing SQL Server and Cisco TMS database.
    a. *If an existing database connection is found*, the existing Cisco TMS database is used. When prompted, enter the username and password to connect to the existing SQL server and click **Next**. Go to step 2.
    b. *If no existing Cisco TMS database connection is found*, the installer looks for a local SQL server. If one is found, enter the username and password necessary to access the server and allow the installer to create a new Cisco TMS database. Click **Next** and go to step 4.
    c. *If no existing Cisco TMS database connection or local SQL server is found*, MS SQL Server 2008 Express 32 bit is installed and a new Cisco TMS database is created. When prompted, enter a password for the sa account (administrator). Click **Next** and go to step 4.

Note: Be sure to note the sa password somewhere secure as it is required for future upgrades and Cisco TMS maintenance.

Note: If the Cisco TMS server is in a domain or you have a local policy that has a strong password policy, ensure that you use a strong password for the SQL installation.



Enter the User Name and password for the SQL Server

A SQL Server has already been installed on this server. Enter a username and a password that has admin rights to the SQL Server.

SQL Server Name: (local)\SQLTMS

User Name: sa

Password:

Figure 2 SQL server user name and password.

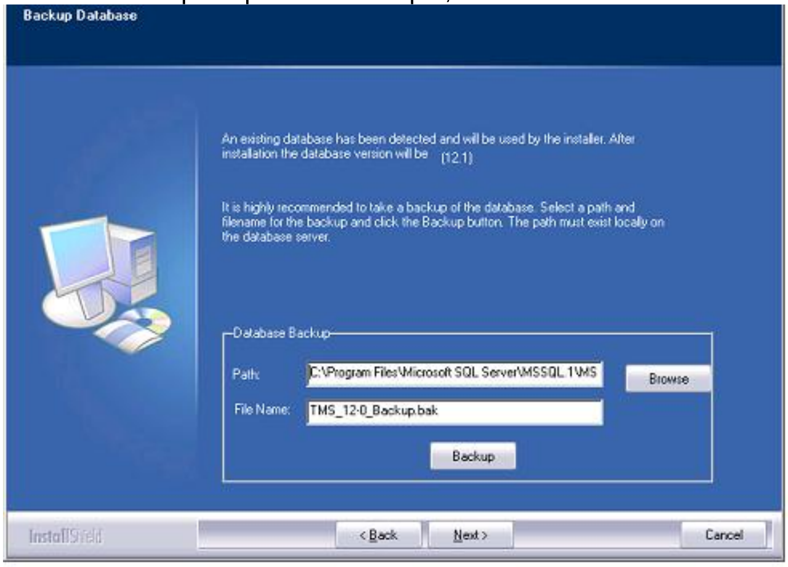
9. You can re-use the existing database:

- To update the existing database to a current version and retain existing information, click **Yes**. Go on to the next step.
- If you wish to install a new Cisco TMS database, then manually remove the existing database from the SQL server, click **No** to abort the install.

10. Cisco TelePresence recommends that you take a backup of your existing database.

- To perform the backup, 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.) Click **Backup** to start the backup. When the backup is complete (it may take several minutes), click **Next**.

- The backup is optional. To skip it, click **Next.**



Backup Database

An existing database has been detected and will be used by the installer. After installation the database version will be (12.1)

It is highly recommended to take a backup of the database. Select a path and filename for the backup and click the Backup button. The path must exist locally on the database server.

Database Backup

Path: C:\Program Files\Microsoft SQL Server\MSSQL.1\MS

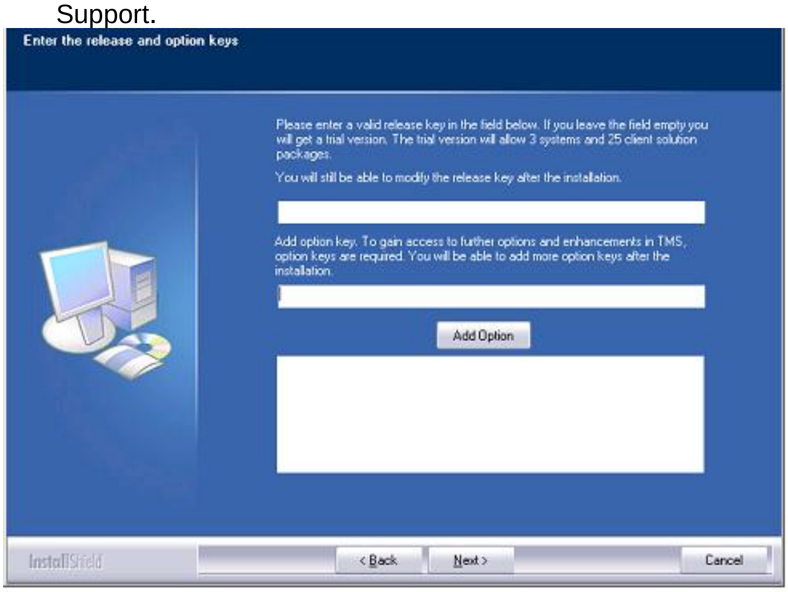
File Name: TMS_12-0_Backup.bak

Figure 3 Backup database.

Note: The installer automatically places the provisioning database (OpenDS) backup in the Cisco TMS backup folder (by default, <TMS folder>\wwwTMS\Data\Backup\opends).

11. If you are upgrading, the ‘release and option keys page’ is displayed and any existing keys are shown. Enter the key(s) to enable additional systems or feature support, such as Network Integration or other external integration packages. A new release key is also required when upgrading to a new major release. The release key must be entered before adding option keys.

    For questions regarding release or option keys, contact your reseller or Cisco TelePresence Support.



Enter the release and option keys

Please enter a valid release key in the field below. If you leave the field empty you will get a trial version. The trial version will allow 3 systems and 25 client solution packages.

You will still be able to modify the release key after the installation.

Add option key. To gain access to further options and enhancements in TMS, option keys are required. You will be able to add more option keys after the installation.

Figure 4 Release and option keys.

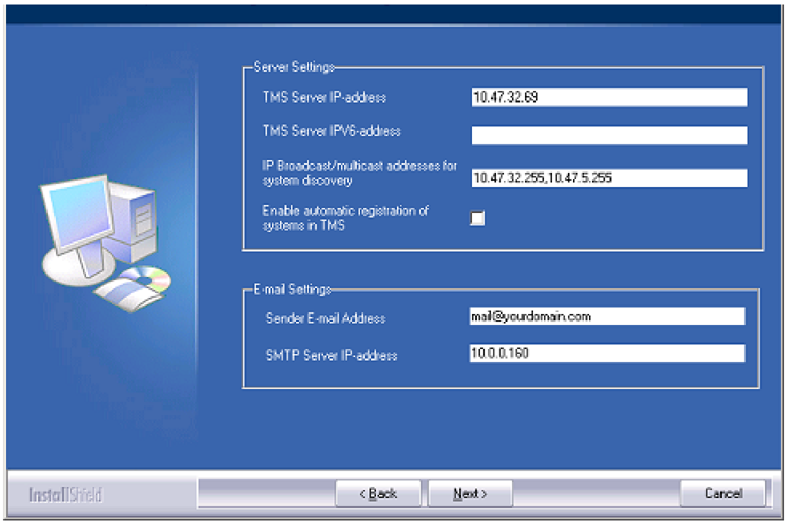
(If no release key is entered, Cisco TMS installs an evaluation version which includes support for three systems, twenty-five clients for Cisco TMS, and Cisco TMS Scheduler.)

To add an option key, click **Add Option** and enter the key. Keys are validated before being added. (Option keys can also be added post-installation via Administrative Tools.) Click **Next**.

You can now configure a range of default settings that allow Cisco TMS to immediately start working with a basic network configuration (these settings can be amended after installation). After configuration, Cisco TMS can automatically discover, monitor, log, provide phone books, and schedule a basic existing H.323/SIP network.

Customizing Cisco TMS is covered in the Cisco TMS user guide, available via the question mark icon (?) on the Cisco TMS client.

12. The Network Settings screen is displayed with values from the existing database (if appropriate). Cisco TMS contacts the supplied SMTP Server to verify the settings and warns you if it was unable to contact the server.



Server Settings

TMS Server IP-address: 10.47.32.69

TMS Server IPV6-address:

IP Broadcast/multicast addresses for system discovery: 10.47.32.255,10.47.5.255

Enable automatic registration of systems in TMS: □

E-mail Settings

Sender E-mail Address: mail@yourdomain.com

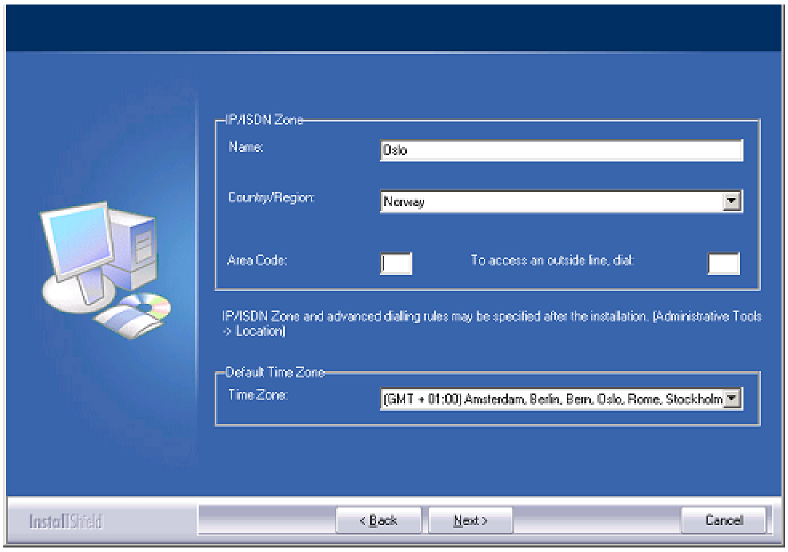
SMTP Server IP-address: 10.0.0.160

Figure 5 Network Settings.

- **TMS Server IP Address** – the IP address of the local server.
- **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 […]** – Cisco TMS will automatically search these networks for devices using these broadcast address(es). (The management settings of systems that Cisco TMS discovers can be automatically). For multiple broadcast addresses, separate each entry with a comma. Cisco TMS will search any networks by sending a SNMP Discovery packet to the supplied addresses. The default value will be the broadcast address of the Cisco TMS server network.
- **Enable automatic registration of systems in 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. The default value is *Disabled*.
- **Sender Email Address** – Enter the mail address you wish to appear as the 'FROM' mail address in emails sent by Cisco TMS. Example: videomanagement@company.com
- **SMTP Server IP Address** – The network address of the SMTP server that Cisco TMS will use to send emails. If necessary, additional authentication settings can be configured after installation.

13. Change the settings as required and then click **Next**.

Zones are a Cisco TMS configuration concept used to route phone numbers and aliases when scheduling calls and using phone books. The information entered creates the first IP Zone and ISDN zone, and the default value to allow a basic IP network to operate immediately after installation. Additional zones can be added post-installation for networks with multiple locations or more complex elements.



IP/ISDN Zone
Name: Oslo
Country/Region: Norway
Area Code:
To access an outside line, dial:

IP/ISDN Zone and advanced dialling rules may be specified after the installation. (Administrative Tools -> Location)

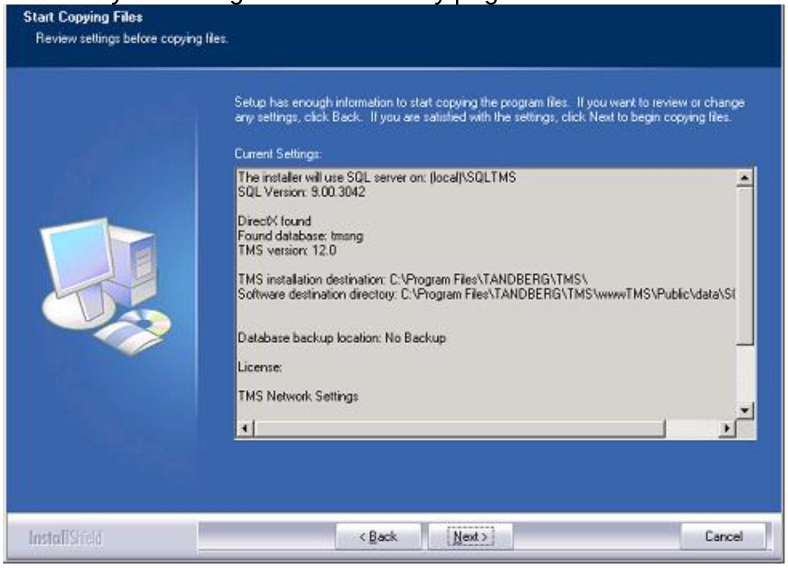
Default Time Zone
Time Zone: (GMT + 01:00) Amsterdam, Berlin, Bern, Oslo, Rome, Stockholm

Figure 6 IP zone and ISDN zone.

- **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 (if applicable) for the location. This is used for ISDN dialing information.
- **To access an outside line [..]** – The prefix (if any) to reach an outside line on your ISDN circuits. This is used for ISDN dialing information.
- **Default Time Zone** – Select the default time zone for new systems and users. Specific settings for each user or device can be changed later.

Complete the Zone information and click **Next**.

14. Verify all settings in the summary page and click **Next**.



Start Copying Files
Review settings before copying files.

Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:

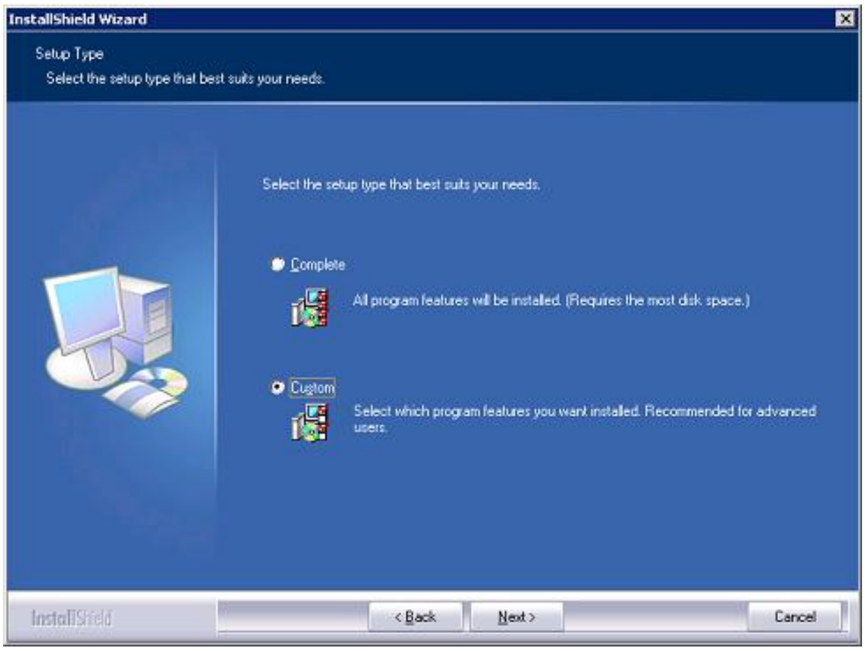
```
The installer will use SQL server on: (local)\SQLTMS
SQL Version: 9.00.3042

DirectX found
Found database: tmsng
TMS version: 12.0

TMS installation destination: C:\Program Files\TANDBERG\TMS\
Software destination directory: C:\Program Files\TANDBERG\TMS\wwwTMS\Public\data\S


Database backup location: No Backup

License:

TMS Network Settings
```

Figure 7 The summary page.

This completes the installation of the Cisco TMS software. Go to the online Cisco TMS user guide, available via the question mark icon (?) on the Cisco TMS client, for further configuration and user information.

Custom installation process

Follow the process in this section if you chose ‘Custom’ for your installation type.



InstallShield Wizard

Setup Type

Select the setup type that best suits your needs.

Select the setup type that best suits your needs.

○ Complete

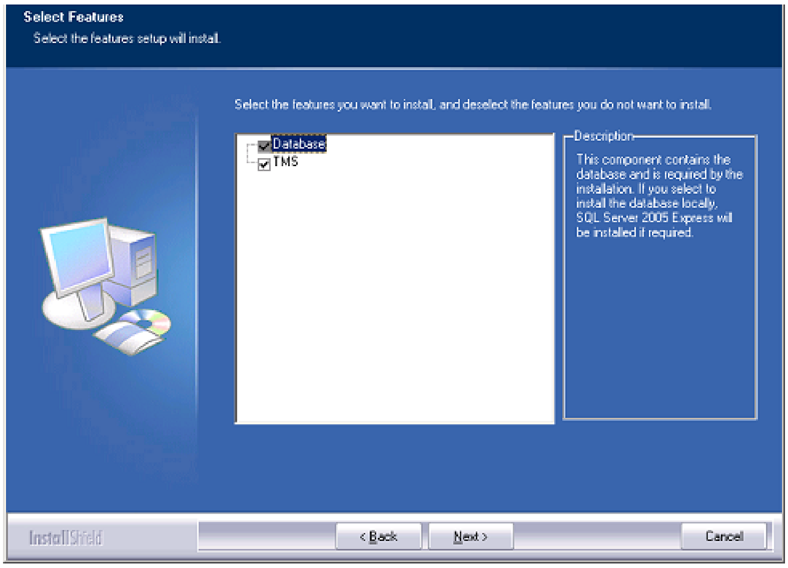
All program features will be installed. (Requires the most disk space.)

● Custom

Select which program features you want installed. Recommended for advanced users.

Figure 8 Custom installation type.

1. You are prompted to select features. Deselecting Cisco TMS means that only MS SQL Server 2008 Express 32 bit and the Cisco TMS database, if needed, will be installed. Choose which components to install and click **Next**.



Select Features

Select the features setup will install.

Select the features you want to install, and deselect the features you do not want to install.

☑ Database
☑ TMS

Description

This component contains the database and is required by the installation. If you select to install the database locally, SQL Server 2005 Express will be installed if required.

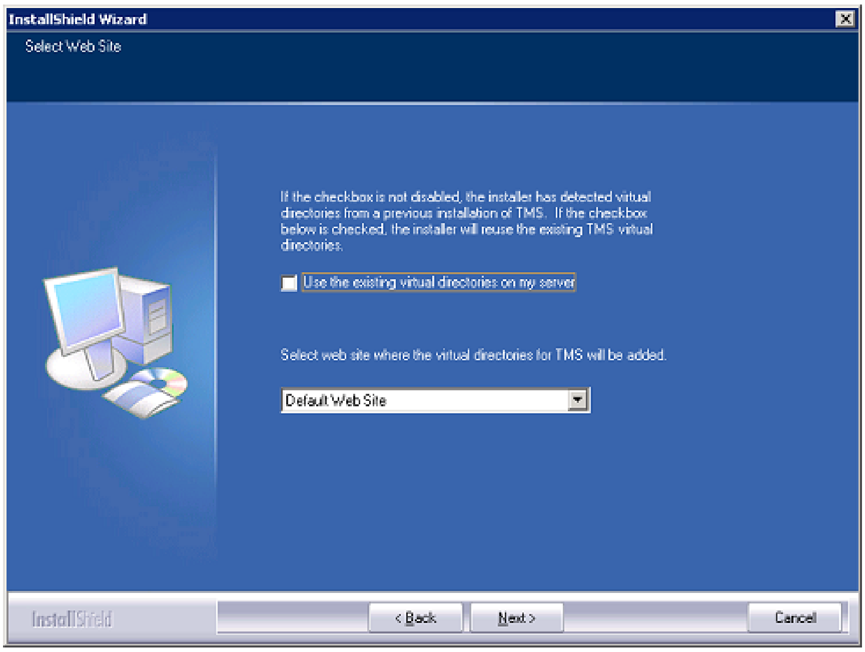
Figure 9 Select features.

2. The installer detects previously used Cisco TMS virtual directories within the IIS server. If you wish to reuse them, select the ‘Use the existing virtual directories on my server’ check box entitled. If there are no existing virtual directories used by Cisco TMS on the server, the check box is disabled.

Note: To be able to use Cisco TMS on a Web Site, it must be accessible by its own IP Address on port 80. Some functionality requires Cisco TMS to be reachable by hostname therefore the web site is also accessible by a fully qualified hostname.

By default Cisco TMS installs itself by creating a virtual directory in the Default Web Site.

Select the Web Site to install to from the drop-down menu and click **Next.**



InstallShield Wizard

Select Web Site

If the checkbox is not disabled, the installer has detected virtual directories from a previous installation of TMS. If the checkbox below is checked, the installer will reuse the existing TMS virtual directories.

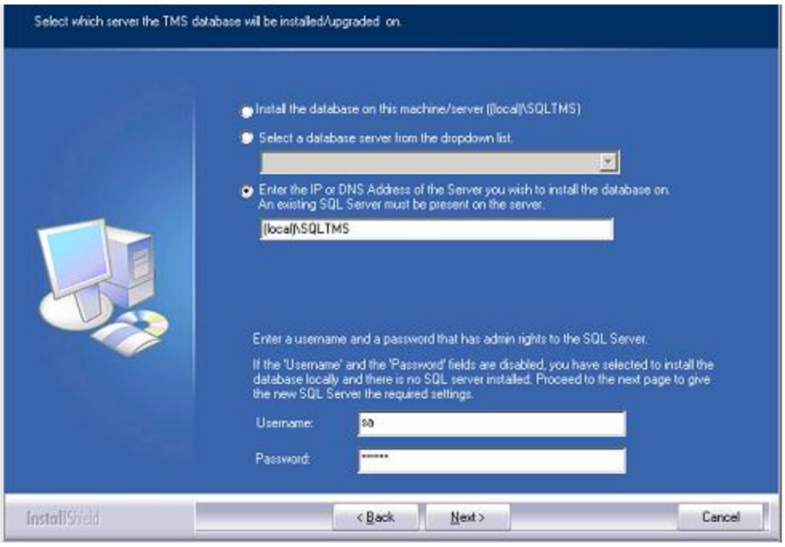
□ Use the existing virtual directories on my server

Select web site where the virtual directories for TMS will be added.

Default Web Site

Figure 10 Select the Web Site.

3. You are prompted to select which server to install on.



Select which server the TMS database will be installed/upgraded on.

○ Install the database on this machine/server ((local)\SQLTMS)

○ Select a database server from the dropdown list.

● Enter the IP or DNS Address of the Server you wish to install the database on. An existing SQL Server must be present on the server.

(local)\SQLTMS

Enter a username and a password that has admin rights to the SQL Server.

If the 'Username' and the 'Password' fields are disabled, you have selected to install the database locally and there is no SQL server installed. Proceed to the next page to give the new SQL Server the required settings.

Username: sa

Password: ******

Figure 11 Select which server.

- **Install Database on this machine… (instance name)** – 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 If no local installation is found, MS SQL Server 2008 Express 32 bit is installed.
- **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

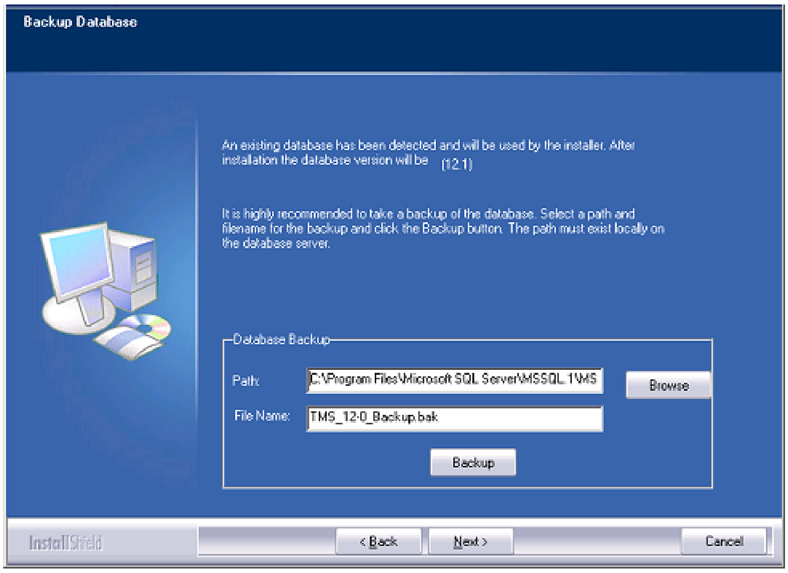
the standard Microsoft SQL conventions to specify named instances, for example: `SQL1.company.com\vidgrp`. If you are unsure of what to enter for your existing SQL server, ask your SQL Server Administrator.

If you selected an existing SQL Server, enter the SQL login information. The specified user is used to create and/or access the Cisco TMS database. Enter the username and password and click **Next**.

If you are installing a new SQL Server locally, these fields are disabled and a separate page 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. Review the SQL guidelines 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. If an existing database is found, Cisco TelePresence recommends that you back it up before upgrading.

   Enter a path for the backup file and filename or click **Browse** to navigate to a folder. The backup is performed on the SQL Server itself, so these values are local to the SQL Server. Then click **Backup.** This may take several minutes. When complete, click **Next**.



Backup Database

An existing database has been detected and will be used by the installer. After installation the database version will be (12.1)

It is highly recommended to take a backup of the database. Select a path and filename for the backup and click the Backup button. The path must exist locally on the database server.

Database Backup

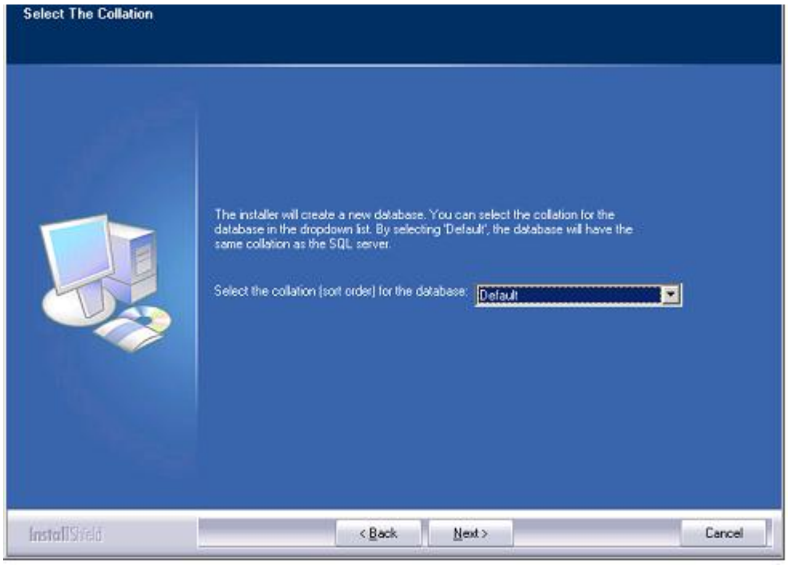
Path: C:\Program Files\Microsoft SQL Server\MSSQL.1\MS

File Name: TMS_12-0_Backup.bak

Figure 12 Backing up Cisco TMS.

Note: The installer places the provisioning database (OpenDS) backup in the Cisco TMS backup folder (by default <TMS folder>\wwwTMS\Data\Backup\opends).

6. If the selected SQL server does not contain a Cisco TMS database, select a collation for the new Cisco TMS database. By default the collation is the same as the SQL server.



Select The Collation

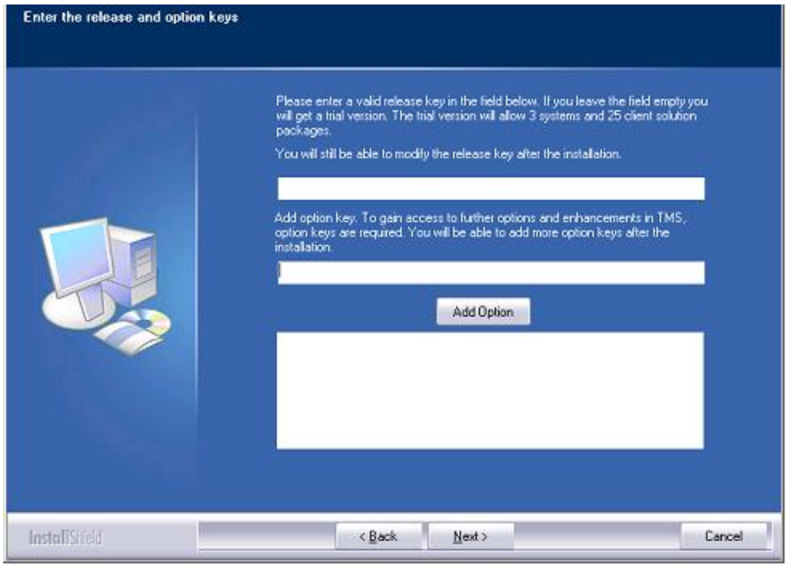
The installer will create a new database. You can select the collation for the database in the dropdown list. By selecting 'Default', the database will have the same collation as the SQL server.

Select the collation (sort order) for the database: Default

Figure 13 Database collation.

7. The Release and option keys page is displayed if you are upgrading, the existing keys are shown. Enter the key(s) to enable additional systems or additional feature support such as Network Integration or other external integration packages. A new release key is also required when upgrading to a new major release. The release key must be entered before adding option keys. To add an option key, click **Add Option** and enter the key. Keys are validated before being added. (Option keys can also be added post-installation go to Administrative Tools.) Click **Next**.

   For questions regarding your release or option keys, contact your reseller or Cisco TelePresence Support.



Enter the release and option keys

Please enter a valid release key in the field below. If you leave the field empty you will get a trial version. The trial version will allow 3 systems and 25 client solution packages.

You will still be able to modify the release key after the installation.

Add option key. To gain access to further options and enhancements in TMS, option keys are required. You will be able to add more option keys after the installation.

Figure 14 Release and option keys.

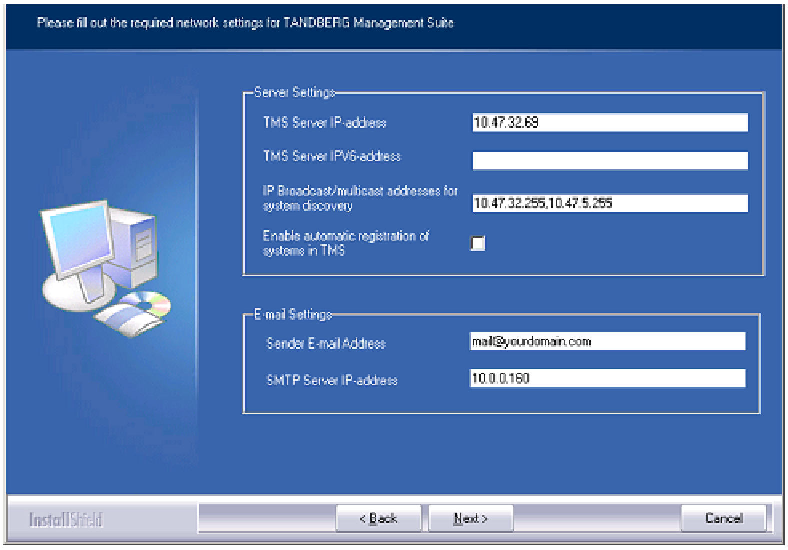
If no release key is entered, Cisco TMS installs an evaluation version of Cisco TMS which includes support for 3 systems for Cisco TMS and Cisco TMS Scheduler.

Your release key must be entered before you add Option keys. Click **Add Option** and enter the key. Keys are validated before being added to the list.

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

Tuning the installation or configuring Cisco TMS for more advanced networks is covered in the Getting Started section later in this document.

8. The Network Settings screen is displayed with the values from the existing database, if appropriate. Complete the settings and click **Next**.



Please fill out the required network settings for TANDBERG Management Suite

Server Settings

TMS Server IP-address: 10.47.32.69

TMS Server IPV6-address:

IP Broadcast/multicast addresses for system discovery: 10.47.32.255,10.47.5.255

Enable automatic registration of systems in TMS: □

E-mail Settings

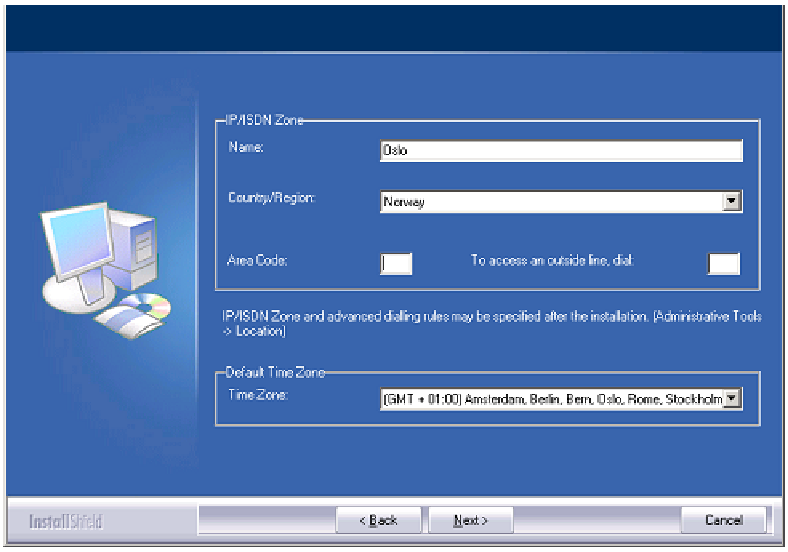
Sender E-mail Address: mail@yourdomain.com

SMTP Server IP-address: 10.0.0.160

Figure 15 Network Settings.

- **TMS Server IP Address** – The IP address of the local server. It will be populated automatically if possible.
- **TMS Server IPV6 Address** – The IPv6 address of the local server. It will be populated automatically if possible. If IPv6 is not enabled on the Windows Server, this field can be left blank.
- **IP Broadcast Address […]** – Enter the broadcast address for the networks 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. The default value is the broadcast address of the Cisco TMS server network.
- **Enable automatic registration of systems in TMS** – Select to have systems that Cisco TMS discovers on the network automatically added into a folder in Cisco TMS and have their management settings configured.
- **Sender Email Address** – Enter the email address that want as the 'FROM' mail address in emails sent by Cisco TMS. For example: videomanagement@company.com
- **SMTP Server IP Address** – Enter the network address of the SMTP server Cisco TMS will use to send emails. If needed, additional authentication configuration settings can be set up post-installation. TMS contacts the supplied SMTP Server to verify the setting and warns you if it was not able to contact the server.

9. Zones are a Cisco TMS configuration concept Cisco TMS used to route Phone numbers and aliases when scheduling calls and using Phone books. The information entered creates the first IP Zone and ISDN zone in Cisco TMS, which will be the default to allow a basic IP network to operate immediately after installation. Additional zones and configurations are added post-installation for networks with multiple locations or more complex elements .



IP/ISDN Zone

Name: Oslo

Country/Region: Norway

Area Code:

To access an outside line, dial:

IP/ISDN Zone and advanced dialing rules may be specified after the installation. (Administrative Tools -> Location)

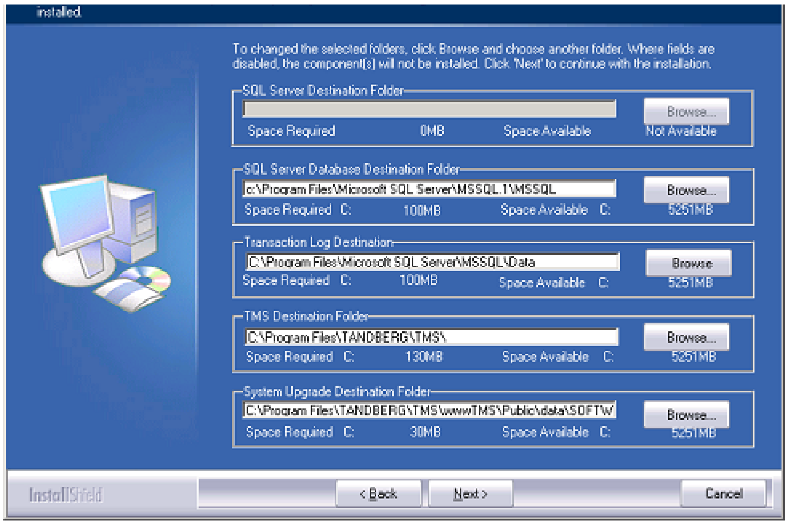
Default Time Zone

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

Figure 16 IP Zone and ISDN zone.

- **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 (if applicable) for the location. This is used for ISDN dialing information.
- **To access an outside line [..]** – The prefix (if any) to reach an outside line on your ISDN circuits. This is used for ISDN dialing information.
- **Default Time Zone** – Select the default time zone for new systems and users. Specific settings for each user or device can be changed later.

10. Complete the Zone information and click **Next**.
11. 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 grayed.



installed

To changed the selected folders, click Browse and choose another folder. Where fields are disabled, the component(s) will not be installed. Click 'Next' to continue with the installation.

SQL Server Destination Folder

Space Required 0MB Space Available Not Available

SQL Server Database Destination Folder

c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL

Space Required C: 100MB Space Available C: 5251MB

Transaction Log Destination

C:\Program Files\Microsoft SQL Server\MSSQL\Data

Space Required C: 100MB Space Available C: 5251MB

TMS Destination Folder

C:\Program Files\TANDBERG\TMS\

Space Required C: 130MB Space Available C: 5251MB

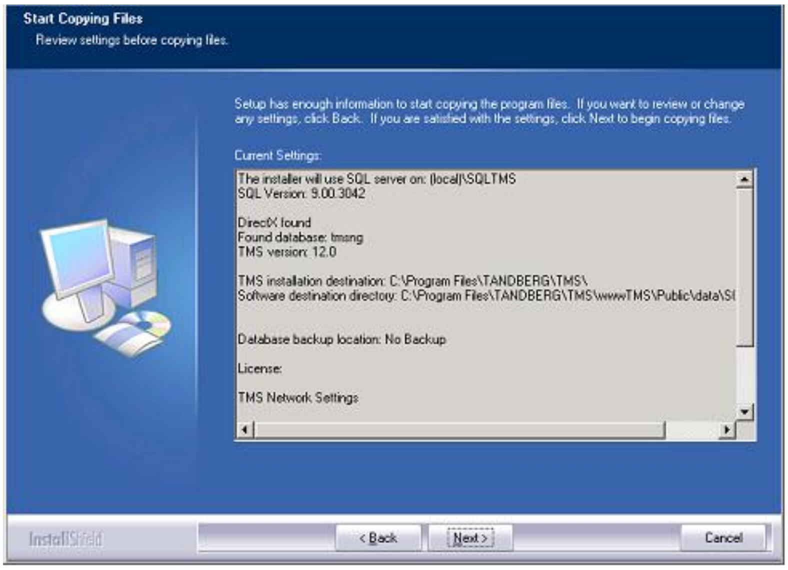
System Upgrade Destination Folder

C:\Program Files\TANDBERG\TMS\wwwTMS\Public\data\SOFTW

Space Required C: 30MB Space Available C: 5251MB

Figure 17 Specify Installation paths.

12. Verify the information on the Summary page and click **Next**.



Start Copying Files

Review settings before copying files.

Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:

```
The installer will use SQL server on: (local)\SQLTMS
SQL Version: 9.00.3042

DirectX found
Found database: tmsng
TMS version: 12.0

TMS installation destination: C:\Program Files\TANDBERG\TMS\
Software destination directory: C:\Program Files\TANDBERG\TMS\wwwTMS\Public\data\S(


Database backup location: No Backup

License:

TMS Network Settings
```

Figure 18 Verify information on the Summary page.

This completes the installation of the Cisco TMS software. Go to the online Cisco TMS user guide, available via the question mark icon (?) on the Cisco TMS client, for further configuration and user information.

Configuring the Cisco TelePresence Management Server

The Cisco TelePresence Management Server Appliance is delivered with Cisco TelePresence Management Suite (Cisco TMS) pre-installed so that you can deploy Cisco TMS without having to buy, configure, or install your own server and operating system. The Cisco TelePresence Management Server Appliance is intended for small to medium sized networks (up to 100 managed systems).

Note: If the Cisco TMS Agent is to be utilized on the Cisco TelePresence Management Server, Cisco TelePresence recommends a limit of 5000 users in the Provisioning Directory.

This section has three topics

- Initial setup and configuration of the
- Operation, maintenance, and upgrading the
- TMS software installation/upgrades on the Cisco TelePresence Management Server

For information regarding the configuration of the Cisco TelePresence Management Server Appliance, see the Cisco TMS Administrator Guide.

- Initial setup and configuration of the Cisco TelePresence Management Server

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, the Cisco TelePresence Management Server Appliance is delivered in a special shipping box which contains the following components:

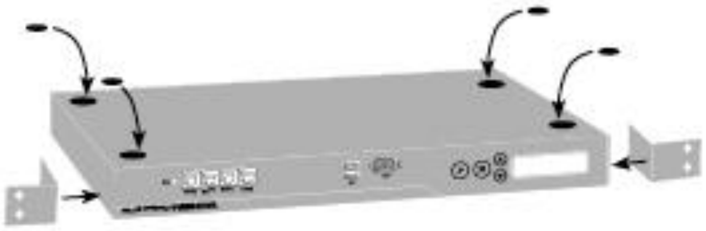
- rack-ears, screws and screwdriver
- cables:
  - power cable
  - Ethernet cable
- Cisco TelePresence Management Server Appliance

Installation site preparations

- Make sure that the Cisco TelePresence Management Server Appliance is accessible and that all cables can be easily connected.
- For ventilation, leave a space of at least 10cm (4 inches) behind the rear panel and 10cm (4 inches) in front of the front panel.
- It is recommended that the room in which you install the Cisco TelePresence Management Server Appliance 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 Cisco TelePresence Management Server Appliance.
- Do not place hot objects directly on top, or directly beneath the Cisco TelePresence Management Server Appliance.
- Use a grounded AC power outlet for the Cisco TelePresence Management Server Appliance.

Rack mounting (optional)

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



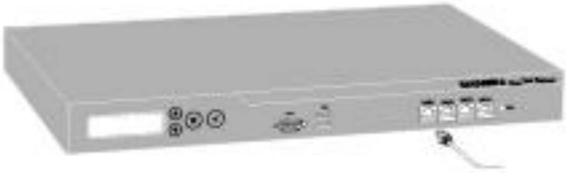
Before starting the rack mounting, ensure the Cisco TelePresence Management Server Appliance is placed securely on a hard flat surface.

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

Connecting cables

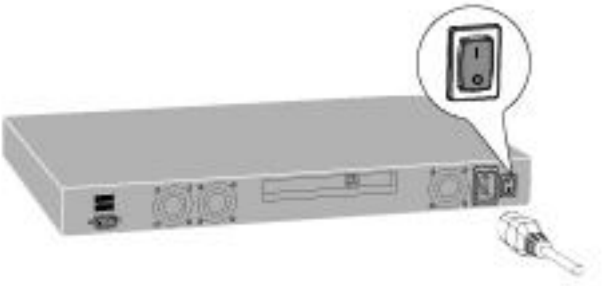
LAN cable

Connect a LAN cable from the ‘LAN 1’ connector on the Cisco TelePresence Management Server Appliance to your network. The LAN 2, 3 and 4 connectors are not used and are 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.



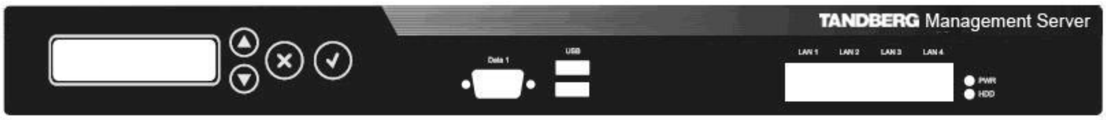
Note: It is recommended that the Cisco TelePresence Management Server is shutdown via the front LCD panel or from the Windows interface before powering the unit off.

Connecting a Monitor and Keyboard (Optional)

Initial network configuration is done via the LCD Panel. After configuration, a VGA monitor, USB keyboard and mouse can be used to access the server console.

IP address configuration

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



LCD Panel buttons and their functions:

▲ ▼	**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 server IP address

15. Power up the server and wait for it to finish booting.
    The LCD Panel will show the current IP of the server after the server has finished starting up.
16. Press **Enter** to display the Main Menu.
17. Use the Up or Down arrow to select **IP Settings**.
18. Press **Enter** to confirm your selection.
19. Use the **Up** or **Down** arrow to select **IP Address** and press **Enter** twice to enter edit mode.
20. 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.
21. 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**.
22. Press **Return** to go back to the **IP Settings** menu.
23. Use the **Up** or **Down** arrow to select **Subnet Mask** and press **Enter** twice.
24. Repeat steps 5-6 to enter the Subnet Mask address.
25. Press **Return** to go back to the **IP Settings** menu.
26. Use the **Up** or **Down** arrow to select **Default Gateway** and press **Enter** twice.
27. Repeat steps 5-6 to enter the Default Gateway address.

Server OS configuration

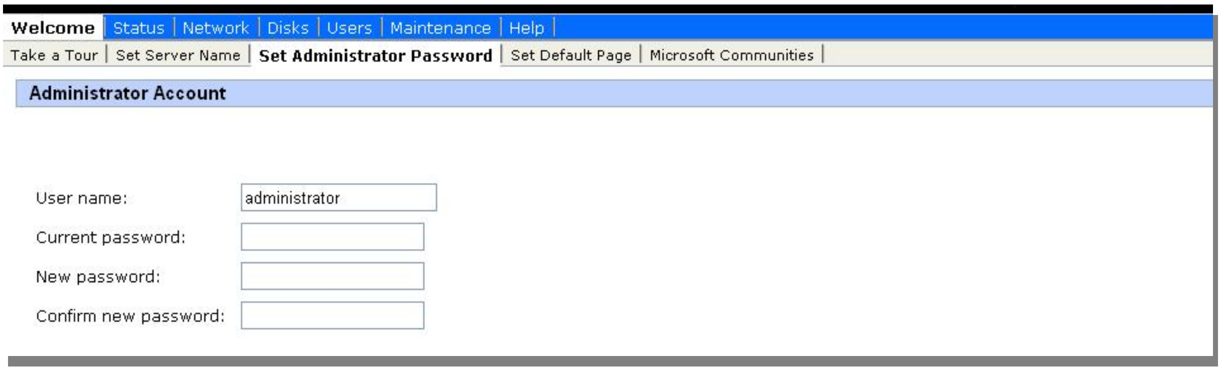
To complete the physical installation of the server, several basic Server OS settings must be configured using the Web User Interface for Microsoft Server. The following steps must be completed from another computer on the network that has Internet Explorer (ActiveX required) installed and network access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

Configuring the server OS

1. In the web browser enter the address **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 pre-installed default server certificate. Click **‘Continue to this website’**.
3. When prompted, enter the username Administrator and password TANDBERG.
4. Change the default administrator password

⚠ Caution: Do not lose your administrator password! Cisco TelePresence 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.

Go to **Welcome > Set Administrator Password**. Set a new password and click **OK** to save the changes. When the change is confirmed, click **OK** to return to the Welcome Screen.


Welcome | Status | Network | Disks | Users | Maintenance | Help |
Take a Tour | Set Server Name | Set Administrator Password | Set Default Page | Microsoft Communities |

Administrator Account

User name: administrator

Current password:

New password:

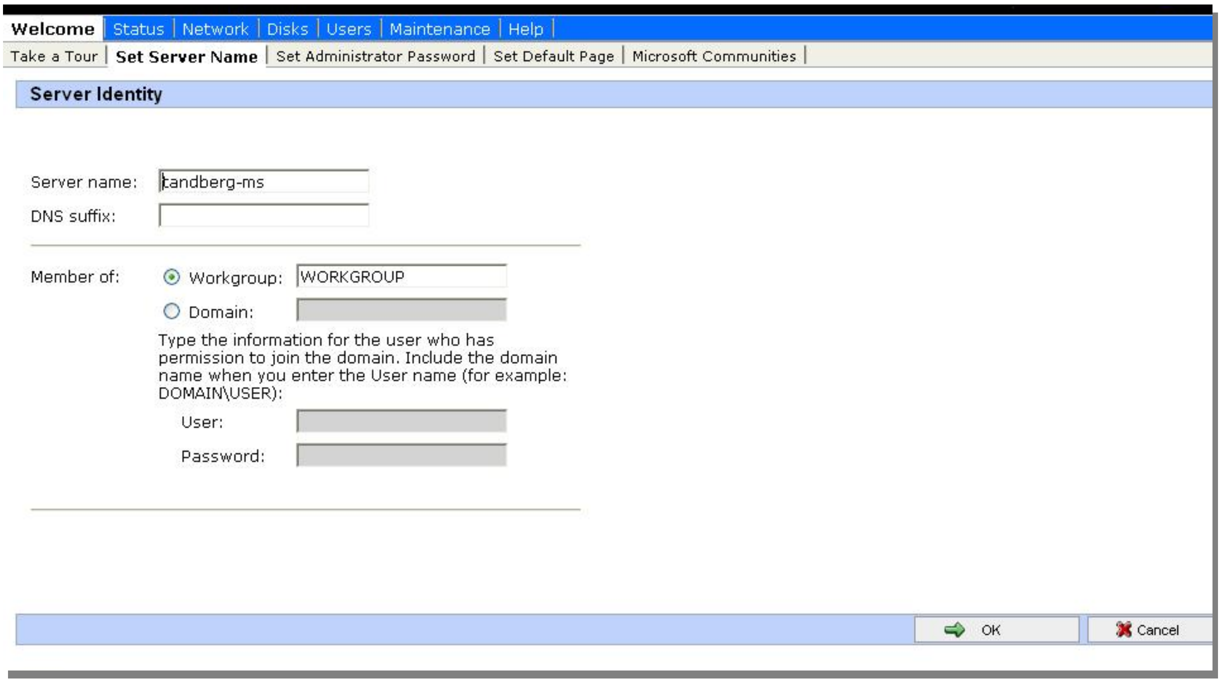
Confirm new password:

Figure 19 Set Administrator Password

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.

5. Set the Server Time and Time Zone: go to **Maintenance > Date/Time**. Update the Time, Date, and Time Zone settings and click the **OK**.
6. Configure the server name and Domain membership and click **OK**:

Go to **Welcome > Set Server Name**.


Welcome | Status | Network | Disks | Users | Maintenance | Help |
Take a Tour | Set Server Name | Set Administrator Password | Set Default Page | Microsoft Communities |
OK
Cancel

Server Identity

Server name: tandberg-ms

DNS suffix:

Member of: ● Workgroup: WORKGROUP

○ Domain:

Type the information for the user who has permission to join the domain. Include the domain name when you enter the User name (for example: DOMAIN\USER):

User:

Password:

Figure 20 Set Server Name.

The default server name is tandberg-ms, but it can be renamed.

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.

WARNING: 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 the Windows Firewall settings all Cisco TMS access to necessary ports. See Ports required by Cisco TMS
9. Ensure that the latest Cisco TelePresence Server Appliance Security Updates are installed.

This completes the installation of the Cisco TMS software. Go to the online Cisco TMS user guide, available via the question mark icon (?) on the Cisco TMS client, for further configuration and user information.

Operation, maintenance, and upgrading the Cisco TelePresence Management Server

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

As with all servers, it is recommended that access to server hardware is restricted and housed in a secure space. It is recommended the server remain on at all times for normal operation.

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

Cisco TelePresence Server Appliance Security Updates

To keep your software current and secure, Cisco TelePresence regularly publishes self-contained security update installers.

Note: For the latest security updates, Cisco TelePresence recommends registering your product. You will automatically be notified when 'Cisco TelePresence Server Appliance Security Updates' become available.

Security updates are available on the Cisco TelePresence web site at:

- http://www.tandberg.com/support/TANDBERG_device_security.jsp
- http://ftp.tandberg.com/pub/software/content_server/security_updates

Note that the Microsoft Windows function Automatic Updates is off by default. This is by design to avoid any untested changes to the underlying Operating System.

It is important that you download and install all security updates from Cisco TelePresence before using this product, and maintain the integrity of all software by applying security and support updates when they become available.

Basic server tasks

Starting and stopping the Cisco TelePresence Management Server Appliance

The Cisco TelePresence Management Server can be restarted and shutdown via the LCD panel. As with all servers, avoid powering off abruptly. It is recommended that restarts/shutdowns 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 the power switch off.

To start up the Cisco TelePresence Management Server:

1. Connect the power and switch the power switch to 1 (on).
   The LCD panel shows the current IP address of the server when the start up process nears completion.

To restart 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. Use the **Up** or **Down** arrow to select **Restart** and press **Enter**.
4. At the *Restart?* prompt, use the **Up** or **Down** arrow to select *Yes* and press **Enter**.

To shutdown 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. Use the Up or Down arrow to select **Shutdown** and press **Enter**.
4. At the *Shutdown?* prompt, use the **Up** or **Down** arrow to select *Yes* and press **Enter**.

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

The system can also be reset and shutdown using Windows Remote Desktop or using the web interface:

1. Start a web browser and enter the address **https://<ManagementServerIPAddress>:8098** where <ManagementServerIPAddress> is the IP address of the Cisco TelePresence Management Server.
2. If you see a security warning stating 'There is a problem with this website's security certificate' – this is normal 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 f, enter the administrator username and password.
4. Select the **Maintenance** tab. Click **Shutdown** then chose to shutdown or restart the server.

Cisco TelePresence Management Server software installation/upgrades

The Cisco TelePresence Management Server is upgraded using the same Cisco TMS Application software (and therefore the same steps) used in software-only installations of Cisco TMS. The Cisco TMS installer automatically detects if the software is being run on a 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 IP or hostname.
2. Login using the local administrator username and password.
3. Copy the Cisco TMS software installer s To the Cisco TelePresence Management Server using a file share, web download, or the drive mapping feature of Remote Desktop Client.
4. Follow the process in the Installation and upgrade section, selecting the **Complete** installation.

Note: The SQL Server sa login information is needed during the upgrade. The SQL login defaults are username: sa and password: TANDBERG.

Note: The Cisco TelePresence Management Server 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 when the Cisco TMS software installer next runs

Getting started with Cisco TMS

This section will help you configure Cisco TMS for first time use and become familiar with some of its tools.

New installations verses upgrades

It is recommended you complete the topics in this section before considering the Cisco TMS installation ‘complete’. During upgrades, these settings are automatically imported into your new Cisco TMS installation. However, Cisco TelePresence recommends that you also review these topics when upgrading to familiarize you with any new feature. A link to the Cisco TMS Release Notes can be found in the References and related documents section.

Getting started topics

This section is broken into two major categories: configuration and orientation. The topics are progressive: later steps rely on the previous steps already being completed. It is recommended a first time administrator complete all the topics in order, then move on to further configuration and/or review the Cisco TMS Administrator Guide for further details.

Configuration topics

Cisco TMS user concepts

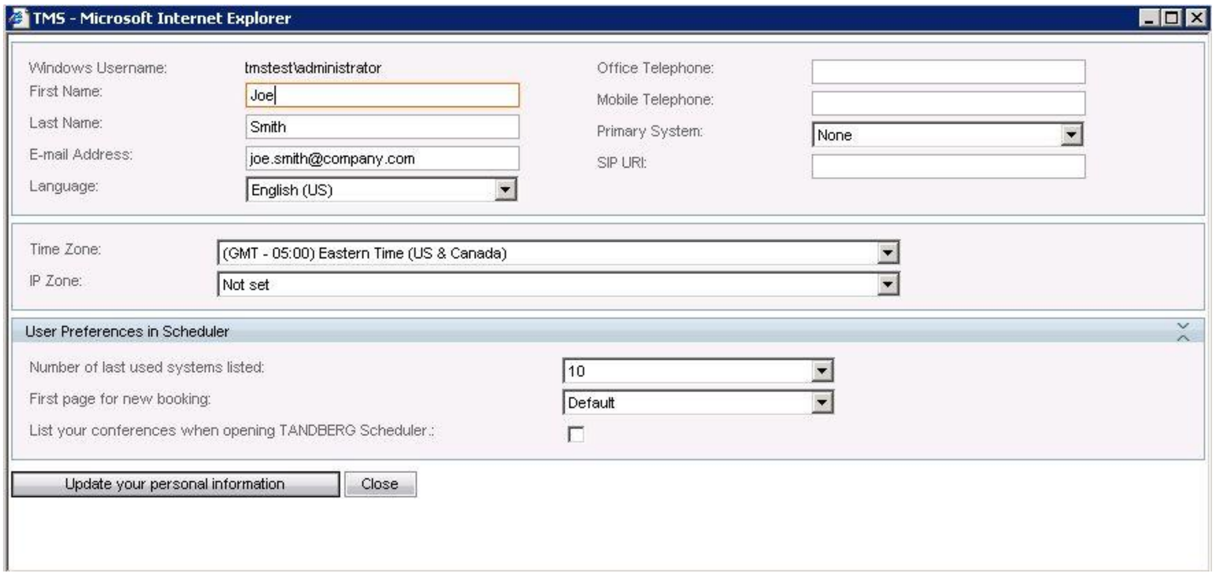
To log into the Cisco TMS web site, you must have a Windows username and password that the server is configured to trust. By default, any local Windows user account will work, as well as any Active Directory Domain user account if the server is a member of an Active Directory Domain.

Cisco TMS creates a user profile for each user that successfully logs into Cisco TMS, based on their Windows username. Cisco TMS does not store user passwords – users use their existing Windows password. 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. Likewise, deleting a user profile in Cisco TMS does not alter their Windows User account. A user must always have a valid Windows login to access Cisco TMS.

In each user profile in Cisco TMS there are personal information fields such as their Windows username, their first and last name and their email address. These fields must be completed for each user; otherwise, when the user browses to Cisco TMS, a pop-up window opens prompting them to complete their user profile. Each user can choose the language to use within the Cisco TMS Application from a drop-down list.

Note: While more languages are supported in the Cisco TMS Scheduler and notifications, only English, French, Russian, Japanese, Chinese (Simplified) and Korean are supported in the main Cisco TMS web interface. If another language is selected, pages that do not support this language selection are displayed in English.

As of version 12.61, Cisco TMS is now available in English, French, German, Chinese, Japanese, and Korean.



TMS - Microsoft Internet Explorer

Windows Username: tmstest\administrator
First Name: Joe
Last Name: Smith
E-mail Address: joe.smith@company.com
Language: English (US)

Office Telephone:
Mobile Telephone:
Primary System: None
SIP URI:

Time Zone: (GMT - 05:00) Eastern Time (US & Canada)
IP Zone: Not set

User Preferences in Scheduler

Number of last used systems listed: 10
First page for new booking: Default
List your conferences when opening TANDBERG Scheduler.: □

Figure 21 A user profile in Cisco TMS.

The remaining fields are not mandatory. If you are using Active Directory, you can configure Cisco TMS to populate these fields automatically for new users; their profile will be created automatically the first time the user logs into Cisco TMS.

Accessing Cisco TMS for the first time

Cisco TMS is accessed via a web browser - **http://<serveraddress>/TMS** where <serveraddress> is the IP Address or hostname of your server.[1]

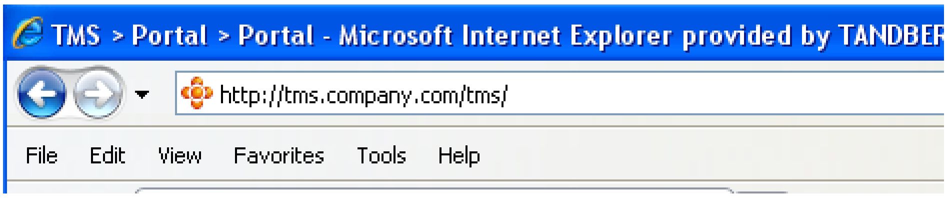

TMS > Portal > Portal - Microsoft Internet Explorer provided by TANDBER
http://tms.company.com/tms/
File
Edit
View
Favorites
Tools
Help

Figure 22 The IP Address or hostname of your server

If you are accessing the web site from the server console, you will be authenticated automatically with your current username. If this fails, you will be prompted to enter your username and password.

Most browsers display two fields in the login window -- a username and password field. How you enter your username depends on the type of Windows account that you are using:

Domain Users[2]	Enter username as: domain\username Example: corp\joe.smith
Local Windows Accounts	Enter username as: machinename\username Example: TMS-2\administrator

The User Profile window is displayed after you authenticate. If not, look for any Pop-Up blocker alerts, and disable pop-up blocking for the Cisco TMS web site.

Fill in the details of the user profile and click **Update Your Personal Information**.

Moving around Cisco TMS and the TMS GUI

Being the first user to log into Cisco TMS, you are automatically an administrator and have full access to Cisco TMS. Functionality is grouped by the main categories across the top of the page.

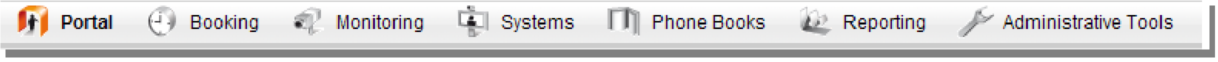
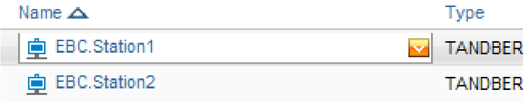


Figure 23 Cisco TMS functionality categories.

Navigating around Cisco TMS is usually done with these top menu items. Hovering over a menu expands it to show the options. Items with triangles next to their name have additional items under that item. Click on an item to jump to that page. The Cisco TMS Sitemap under the Portal menu is a single page with links to all the pages in Cisco TMS: the Sitemap is a quick way to find a page if you are unsure of its location.

Using your mouse with the top menu items is just one example where the mouse hover is used. Hovering over an item may display additional tips or information about the item in a tooltip. In other pages, hovering displays the option for a drop-down menu. Clicking the orange icon opens a menu to interact with that individual item.



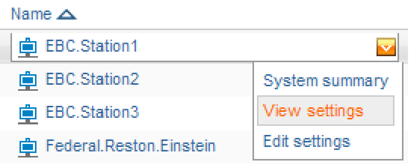


Figure 24 Drop down available

[1] Using the server hostname is recommended because, when used with Active Directory accounts and a compatible setup, Integrated Authentication allows a user to log in without having to re-enter their Windows username and password.

[2] The username@'Domain DNS name' format is also suitable, but less commonly used

Figure 25 Drop down activated

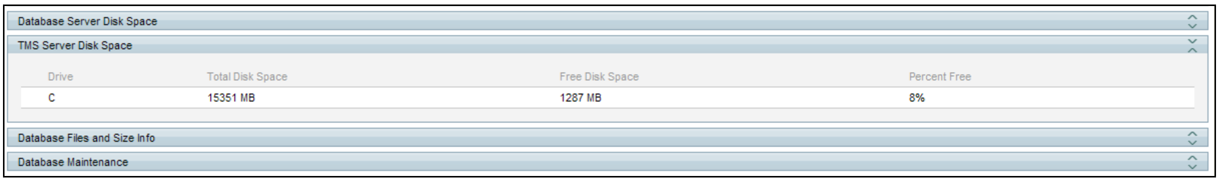
The order of items in most lists in Cisco TMS can be changed by clicking the column title. How a list is currently sorted is indicated by a small triangle: in the image above, the list is being sorted by the Name column in ascending order. Clicking on ‘Name’ would change the list to descending name order, clicking on ‘Type’ would change the list to sort by device Type.

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 ‘paged’, and there are Previous and Next links at the bottom of the list. Use these to page through long lists. Some lists also have search and filter options to control what information is displayed to help you find what you are looking in large amounts of data. Many pages also allow you to control how many rows are shown as a time: the more rows that are shown, the longer it takes to load the web page.

Many pages in Cisco TMS have multiple views or subpages on the same page: shown as tabs across the top of a window. There can be multiple levels of tabs as well.

The above image has multiple pages, including Summary, Settings, Call Status, Phone Book, Connection, etc. Setting, the active tab, is displayed in a darker blue. The Settings tab has additional views under it, including View Settings, Edit Settings, Extended Settings, and Compare Settings. View Settings is the current view and is highlighted therefore.

Another important concept is collapsible panels. A panel has a Blue bar at the top. If the bar has arrow icons at the right edge, clicking on the blue bar collapses or expands the panel. This allows you to choose which areas of the screen to see more of.



Database Server Disk Space

TMS Server Disk Space

Drive	Total Disk Space	Free Disk Space	Percent Free
C	15351 MB	1287 MB	8%

Database Files and Size Info

Database Maintenance

Figure 26 Collapsible blue bar panel.

The top right corner of the Cisco TMS web page has a Search box and a question mark. The search box provides a quick way to find an individual system. You can search by name, phone numbers, serial numbers, and more. This is the quickest way to quickly display more information about a system. The question mark is the help icon: clicking on it displays a new window with the online help page for the open web page.

Permissions and groups in Cisco TMS

Administrators can control which Cisco TMS features users have access to, such as Booking and Device Management, and which systems they can uses those features with. These feature and system permissions combine for an effective ability per system. For example, it is possible to give the IT team in Chicago the ability to fully control and manage endpoints in Chicago, but prevent them from scheduling or making changes to systems in London.

Functions and systems that users do not have access to are normally hidden from them. If a user has no Booking permissions, the Booking Menu is not shown. This allows you to create very simple interfaces for users with a limited role so that they will not be overwhelmed with the full range of features.

Cisco TMS controls permissions through User Groups. Groups are defined in Cisco TMS, and users are assigned to groups. What permissions users have in Cisco TMS is based on which group(s) they are a member of and the permissions that each group has. Permissions in TMS are *cumulative* –the effective permission that a user has is a sum of all the group permissions they belong to.

Groups and permissions are controlled from the User Administration Menu under Administrative Tools. To display or see a group permission go to **Administrative Tools > User Administration > Groups > Set permissions**.

Cisco TMS has several default groups, but the most important groups are the **User** and **Site Administrator** groups:

- All users are always a member of the **User** group, so it is not possible to edit the membership of this group and any permission given to the **User** group is available to all Cisco TMS users.

- 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 because it always has full permissions.

It is recommended administrators define more groups to allow greater control of permissions in Cisco TMS. Which groups users are a member of can be set one of three ways:

- By editing the group itself. The Edit Group page displays all current members: click **Add Members**, to specify which users to add to the group. A user can be a member of more than one group. User groups can also be edited by editing the User, go to **Administrative Tools > User Administration > Users**
- By assigning the user to a group automatically when the user profile is created. Cisco TMS does this through 'Default groups'. Groups set as a 'Default group' are automatically added to any new user. At first installation, the Site Administrator group is marked as a Default group. This means any person who logs into Cisco TMS, has a user profile created, and is automatically be added the Site Administrator group giving them full rights to Cisco TMS. This is how you became an administrator automatically when you first log into Cisco TMS. After you have logged in as the administrator, it is recommended you stop the Site Administrator group from being a Default group; otherwise every user will have full access permissions.
- By using Active Directory Groups. Cisco TMS has the option after configuration to allow Cisco TMS to import existing groups from Active Directory. The Active Directory groups that a user belongs to is automatically updated in Cisco TMS Groups when the user logs in. This simplifies group administration because it reuses the existing Enterprise Directory for groups within Cisco TMS l.

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

At this point, it is important to understand that there are default permissions given to a system when it is first added to Cisco TMS. This is controlled by '**Default System Permissions**' under **Administrative Tools > User Administration > Default System Permissions** which allows you to set the permissions that each group gets by default on newly added systems.

Configure a baseline permissions setup

For initial setup, it is not important to define all your eventual groups, but it is important understand how permissions are set and to establish a baseline of what permissions you want until you settle on a more complete and formal configuration.

As a best practice, the following initial configuration steps must be done so that new users will not have Cisco TMS Administration rights, and you have a default group for new users with a baseline permission set. The permissions can be changed at any time, but it is recommended administrators start planning from the beginning on how access will be controlled and what features users will have access to by default.

1. Create a new group to use for all your trusted users. Go to **Administrative Tools > User Administration > Groups** and click **New**. Enter a name, such as 'All company users' and click **Save**
2. Assign the default permissions that you want all Cisco TMS users to have to the new group. Click on the Group Name in the Edit Group listing, and click **Set Permissions**. Select the check box for each permission that you want group members to have. For a starting point that gives users full access except to Cisco TMS configuration, select all the check boxes except those under Administrative Tools. Use the check boxes in the blue title bars to select or clear all check boxes in that section. Click **Save**
3. Change the Default Groups. Go to **Administrative Tools > User Administration > Default Groups**. Clear all the check boxes except for the Users Group and your new Group. This means any person who logs into Cisco TMS will automatically be added to your new group, and be given the permissions that group has. Click **Save**
4. Change the Default System Permissions. Go to **Administrative Tools > User Administration > Default System Permissions**. You will see that the new group has no permissions, and the User

Group has all permissions. Clear all the check boxes for the User Group, and assign the permissions you want for the new user group. Click **Save**.

5. Ensure only intended users have Site Admin access. Go to **Administrative Tools > User Administration > Groups**. Click on the Site Administrators group and click **Edit**. In the Members list, ensure that only the users you want to have Administrator rights are listed. If any other accounts are listed, select the check box in their row and click **Remove**. Click **Save**

These steps have established a baseline permissions model that:

- Prevents new users from being Site Administrators.
- Setup a ‘baseline’ permissions group.
- Ensures that all new users and systems will have the baseline permissions configured on them by default.

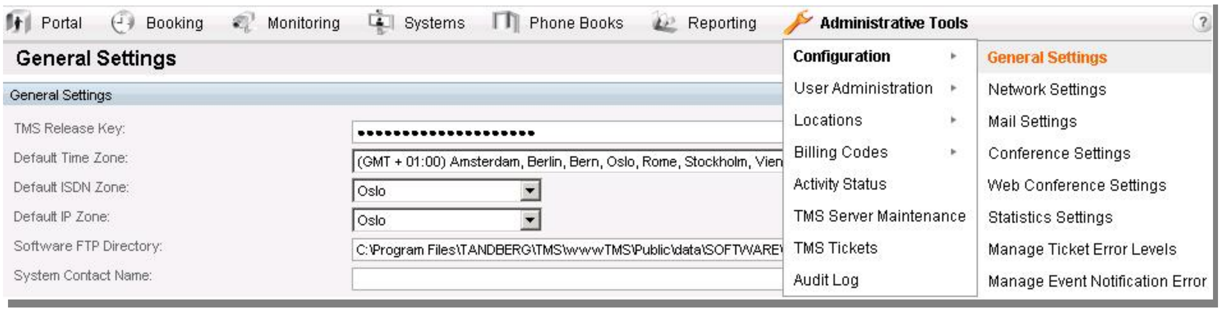
Beyond initial configuration, administrators must plan their Cisco TMS deployment in terms of who they wish to do what in Cisco TMS. This is controlled through Group Membership, Group Permissions, and System Permissions.

Review and set important Cisco TMS defaults

Cisco TMS is highly customizable to meet your organization needs and can be configured at any time. Most settings are configured automatically or have suitable default values. However, there are some important settings to review and configure as part of your initial setup, to ensure that they meet your needs and to simplify the configuration of other Cisco TMS features.

This topic outlines the settings to review and configure at first configuration. For complete details on each setting, see the online help or the Cisco TMS Administrator Guide.

The majority of Cisco TMS configuration settings are controlled from the Administrative Tools menu.



General Settings

General Settings

TMS Release Key: ••••••••••••••••••••

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

Default ISDN Zone: Oslo

Default IP Zone: Oslo

Software FTP Directory: C:\Program Files\TANDBERG\TMS\wwwTMS\Public\data\SOFTWARE\

System Contact Name:

Figure 27 General settings.

Significant **Administrative Tools > General Settings** for review are:

- **System Contact/Email** –When completed, these settings display a Contact link on the bottom of all Cisco TMS pages so that users can easily contact you for help.
- **Enable Auditing** – This setting enables Audit logging that is, configures Cisco TMS to keep detailed logs of all changes to systems, users, and other key elements. The Audit Log is accessible in the Administrative Tools menu. This setting is disabled by default, but security conscious administrators may want to enable it from the outset. But note that enabling this feature causes the Cisco TMS database to grow significantly faster.
- **Release Key/Option Keys** – If you did not enter your release key and option key during installation, you can enter them here. If you are upgrading from a trial version or adding new options, this is where license information is entered.

See Installing licenses documentation for further information on licenses and release keys.

Significant **Administrative Tools > Network Settings** for review are:

- **SNMP Community Name** – This is a comma separated list of common SNMP strings that Cisco TMS uses when discovering and adding systems. 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…** - Enter your email address here so that Cisco TMS can send you notifications about rogue endpoints, system event failures, and for other administrative messages. Multiple email addresses can be entered separated by commas.
- **Automatic System Discovery** – By default this setting is enabled, automatically adds the systems that Cisco TMS discovers to a folder in System Navigator, and configures their management properties to work with Cisco TMS. This makes Cisco TMS very simple to set up. Cisco TMS configures the systems with basic settings from the 'Discovered Systems Template'. Later, if there are default settings you wish all new systems to have, update that template.
- **Active Directory** – These settings allow Cisco TMS to leverage Active Directory for its user and group settings. If the Cisco TMS server is a member of a domain, Cisco TelePresence recommends that 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 automatically populates 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. See the Cisco TMS Administrator Guide for further details on Active Directory Groups.
- **Scan SNMP Capable Systems to Allow…** - This setting allows Cisco TMS to detect when a system goes offline more quickly. Cisco TelePresence recommends that you enable this setting.
- **SNMP Broadcast/MultiCast Address(es)** – The network addresses that were configured in the Cisco TMS installer are displayed. Cisco TMS sends an SNMP query to these addresses to find new systems. If your network spans multiple networks, add the broadcast address for each one, separated by commas to allow Cisco TMS to find systems automatically. Do not worry if all the networks are not represented here because systems can also be added manually and through systems contacting Cisco TMS.
- **Enforce Management Settings…** - This setting is enabled by default and is recommended to ensure that 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. This is used to account for a remote network, such as one outside the organization firewall or proxy that you may have systems on and want to manage[3]. These settings are critical because Cisco TMS must know its own network addresses to properly configure systems to communicate back to Cisco TMS.
- The 'local' or LAN network is normally synonymous with your organization's internal network. The 'public' network is a second network that can access Cisco TMS and is generally used to represent the public internet or a network outside the organization firewall. Each system added in Cisco TMS has a Connectivity parameter that you use to tell Cisco TMS which network identity to use when communicating with that system. The public network addresses are used always used when using the SOHO/Behind Firewall support in Cisco TMS.
- **TMS Server IPv4/IPv6 Addresses** – These addresses were configured during installation and are the IP addresses used to reach your Cisco TMS Server
- **TMS Server Fully Qualified Host Name - Internal LAN** – The fully qualified DNS hostname 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.

[3] TMS is still only connected to one physical LAN port and only one IP Address. TMS does not support multihomed networking. The public hostname used will resolve to a IP forwarded to the IP address of the TMS server.

Note: The Cisco TMS Agent application does not use the fully qualified DNS hostname configured here, although they may/could be the same in a single Cisco TMS environment (recommended). The Cisco TMS Agent uses the actual local hostname of the Cisco TMS server and this must match the DNS A record for the Cisco TMS Agent. In a Cisco TMS redundant setup, the fully qualified DNS hostname configured here must be unique and resolvable to reflect the Cisco TMS redundancy; that is, resolvable to the network load balancer. However, DNS records for each particular redundant Cisco TMS (local hostname) will also need to be created so that the Cisco TMS Agent can resolve and thereby replicate between the TMSs appropriately.

- **TMS Server Address (Fully Qualified Host Name or IPv4 Address) – Public or Behind the Firewall respectively** - This must be the fully qualified DNS hostname used to access your Cisco TMS server from an outside network if that is 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 for new software available for your systems over a secure link, and to notify you of your Service Contract status for your Cisco TelePresence Systems. No personal information is sent during this communication except the system identification 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 its properties here.
- **Secure-Only Device Communication** – This setting is disabled by default and only be enabled in specific instances. See the Implementing Secure Management documentation available on the Cisco TMS installation media for more information.

Significant **Administrative Tools > E-Mail Settings** were configured during the Cisco TMS installation. However, if your mail server requires SMTP Auth to be able to send email, configure an appropriate username and password here. The settings are tested when you click **Save** to ensure that they are valid.

Significant **Administrative Tools > Conference Settings** settings control most of the Cisco TMS behavior for scheduled calls and for monitoring of active calls. Significant settings are:

- **Default Bandwidth** – The default bandwidth suggested for H.323 and SIP calls in Cisco TMS Scheduling.
- **Default ISDN Bandwidth** – The default bandwidth suggested for ISDN calls in Cisco TMS Scheduling
- **Set Conferences as Secure by Default** – Cisco TMS can work with systems that support encryption and those that do not. This setting controls the default behavior for Scheduled Conferences. 'If Possible' is the default setting and enables encryption when all systems in a call support it.

WebEx integration

For WebEx booking to work, the booking user *must* have a WebEx User & Password defined in their Cisco TMS profile. This is done so the correct user 'owns' the meeting in WebEx and can log in and operate the WebEx call.

Early iterations of WebEx used a shared account, which while made booking available to everyone, it was less functional because users did not have the correct permissions on the created WebEx meetings.

Cisco TMS routing and zones

To automate conferencing and increase reliability, Cisco TMS actively manipulates dialing information shown to users and systems by interpreting the status and configuration of systems it is managing and understanding of the network. This reduces the technical details that users need to understand. All of these decisions are handled automatically by Cisco TMS.

This information is defines as Zones, and Cisco TMS uses this configuration information to coordinate and integrate with connected networks. There are IP Zones, and ISDN zones. The administrator defines the zones that represent their network, and then systems in Cisco TMS are automatically associated with the zone. During installation, two Zones are defined named ‘Default’.

These need to be expanded upon to implement a network that goes beyond a single location. Zones are created and managed in Cisco TMS in **Administrative Tools > Locations**.

ISDN zones

ISDN zones define the ISDN network in a location. A location is an area that all has the same ISDN dialing behavior: Therefore, a location could be as small as a building or as large as an entire city or state, but all the systems assigned to a zone must share all the same ISDN dialing information:

- **Country/Region -** Defines which dialing rules to use. For example, do I dial 011 or 00 to dial international calls?
- **Area code** – Allows Cisco TMS to make determinations about long distance dialing.
- **Line prefixes** – Defines any prefix digits – such as dialing 9 to get an outside line from a PBX.
- **Digits to dial for internal calls** – How many digits to dial when making calls between systems in the same ISDN zone. For example, if you are using a PBX, it may only be necessary to dial the last 4 digits between two local systems.
- **Area Code Rules** – Used to further tweak the dialing behavior of Cisco TMS with regards to local and long distance calling.

How many ISDN Zones you need to represent your network depends on how many different ISDN dialing behaviors there are. If systems share the identical settings for the above properties, they can share the same ISDN Zone.

All ISDN numbers in Cisco TMS are stored as ‘fully qualified numbers’; that is, the number is entered and shown as the full number, including its country code information. For example: a US phone number is shown as +1 703 7094281 and a Norwegian phone number is: +47 67125125. By storing numbers in a fully qualified format instead of how one system dials a number, the same number can be used by any system in the world because Cisco TMS (with ISDN Zones) knows how to manipulate the number so that any of the systems it manages can dial it properly.

IP zones

The job of an IP zone is twofold – to create the idea of locality in an IP network, and to provide information for connecting from the IP network using Gateways and URI dialing.

IP Zones are purely logical entities and do not necessarily map to any physical boundary. Cisco TMS uses IP Zones to influence its routing decisions because it relates to distance to answer the question ‘Which system is closer to me?’ Two systems that are both in the same IP Zone would be considered ‘local’ to each other. Locality affects choices such as selecting an MCU – a local MCU may be preferred. IP Zones also provide gateway and dialing information about the network a system is attached to. If an organization does not have widespread IP connectivity between sites, and prefers to use ISDN when making certain connections, that is also controllable through IP Zones.

For most organizations, IP Zones provide gateway information for the IP network. The number of IP Zones needed is based on how many gateway paths there are to the network. For more diverse networks with distributed MCUs, IP Zones can also be used to control which MCU is preferred for different groups of endpoints.

Proper Zone configuration is essential in order for phone books and the scheduling to function properly, therefore an understanding of Zones is essential and it is recommended basic zone configuration be undertaken as part of the initial configuration.

Adding zones for initial configuration

To start a simple network plan:

1. For each system that Cisco TMS will manage initially that has ISDN directly connected to it (including MCUs, Gateways and endpoints), create one ISDN Zone, if necessary. Go to **Administrative Tools > Locations > ISDN Zones** and click **New**. Complete all applicable fields and click **Save**.

   Consider whether an existing zone has the same values. For instance, if you have an MCU, Gateway, and endpoint all in the same building, that all use the same ISDN dialing behaviours, they can all use the same ISDN Zone.

   You can add additional zones subsequently; normally before or after adding a new system
2. For each IP Gateway (gateways that act as a pooled service can be considered as a single gateway), create one IP Zone. Go to **Administrative Tools > Locations > IP Zones**, click **New** and complete all the gateway information that applies, including prefixes and DID numbers. Select the ISDN Zone that applies to the Gateway this zone contains. Click **Save**

   By default, when calling between two different IP Zones, ISDN is preferred, if available. Use the lists at the bottom of the screen to set which zones you prefer to use IP when calling between.

   If you have no Gateways, you still must have at least one IP Zone. A zone named ‘Default’ was created during the installation of Cisco TMS and can be used as your sole IP Zone.
3. Select which Zones to use as the default for newly added systems added to Cisco TMS by Automatic System Discovery. When adding a system manually, this value can be overridden. You can also change a system zone by editing its settings. Go to **Administrative Tools > Configuration > General Settings**. Select the Default ISDN and IP Zone settings and click **Save**.

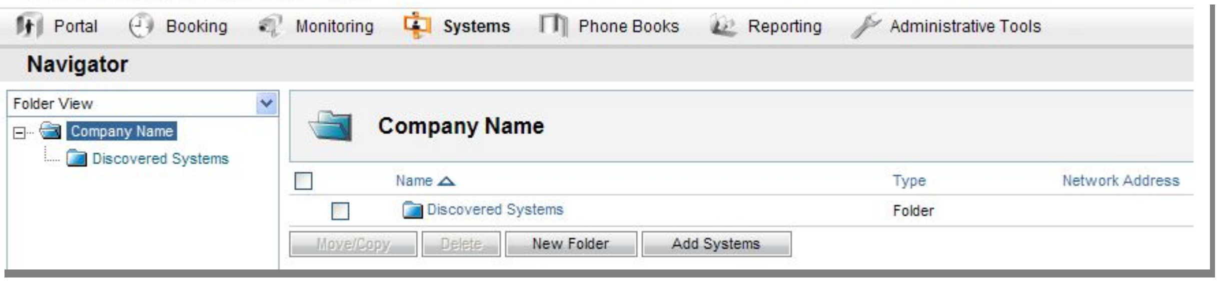
For more assistance with Zones and advanced routing scenarios, see the Cisco TMS Administrator Guide.

Orientation topics

The system navigator

The System Navigator is the starting point for adding, managing, and organizing systems in Cisco TMS. Go to **System > Navigator**. It is where systems are organized into a hierarchal structure of folders, similar to your computer file system. This folder structure, known as the Navigator Tree, is used throughout Cisco TMS when interacting with systems, including the view of systems that users see when Scheduling calls.

In a new installation, two default folders are displayed in the list on the left side of the page: a root (top level) folder called Company Name and a child folder, Discovered Systems. The page is organized into two panels: a tree view on the left, and a details panel on the right which provides information about the selected item on the left.



□	Name	Type	Network Address
□	Discovered Systems	Folder	

Figure 28 Company Name and Discovered Systems.

You can define any folder structure under the root folder, they are purely for organizational purposes to make it easier to find systems and to set system permissions. The same folder structure is seen by all users, and is used throughout Cisco TMS, therefore it is recommended you design a scheme that is meaningful for your users. A common model is one based on geography and organization; for example:

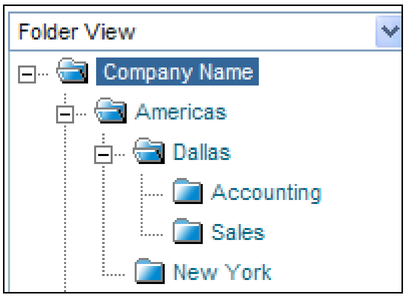


Figure 29 A common geographical organization model

In addition to viewing systems by folder, you can change the tree to display systems by Type, Status, and Manufacturer for example by selecting from the drop-down menu at the top of the tree. However, you can only add, move, or remove systems in the Folder View.

Set up default folders

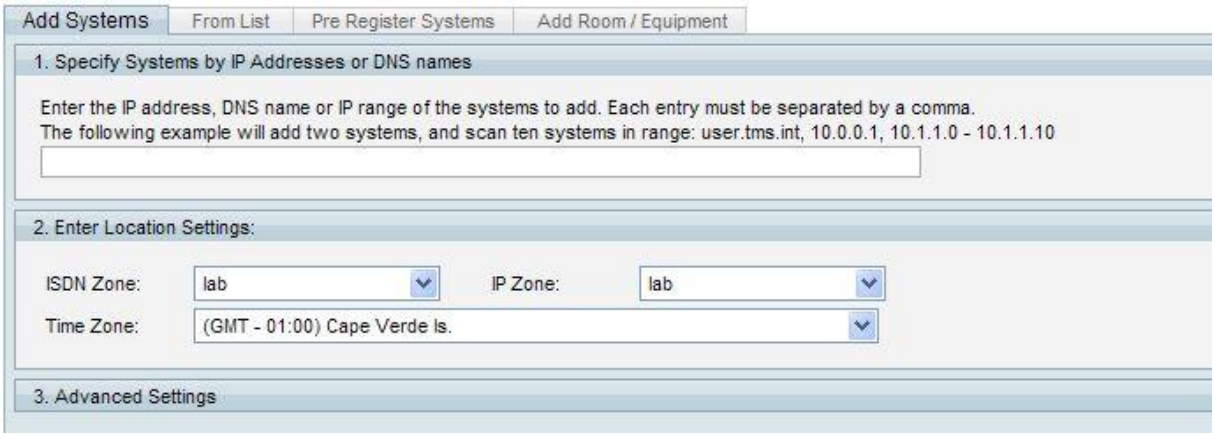
1. Rename the default root folder: click on the Company Name folder. The right panel shows the contents of that folder. Click **Edit this Folder** at the top right-hand side of the screen. Rename the folder with an appropriate company name and click **Save**.
2. Add any additional folders. Folders are not required, but are recommended for organizational reasons. You can always add/remove folders subsequently. To add a folder, click on the folder that will be its parent folder in the tree. Then in the right panel, click **Make New Folder**. Enter a name and description (optional), and click **Save**.
3. Repeat the previous step for as many folders as required.

Adding a system

To manage a system, it must first be added to Cisco TMS. As part of your installation, Automatic System Discovery was enabled, and Cisco TMS may have already added some systems to the Discovered Systems folder. Click on the Discovered Systems folder to display these systems in the right panel.

To add a system, it must be online and you need to know its network address (IP Address or Hostname) and any passwords or SNMP Community names. Some system types or systems that have been locked down for security reasons may require some configuration before being added to Cisco TMS. The examples below assume you are adding a Cisco TelePresence endpoint: see the Cisco TMS Product Support document for full details for each type of system.

1. Navigate to the parent folder and click **Add Systems** in the right panel.



1. Specify Systems by IP Addresses or DNS names

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

2. Enter Location Settings:

ISDN Zone: lab
IP Zone: lab
Time Zone: (GMT - 01:00) Cape Verde Is.

3. Advanced Settings

Figure 30 The Add Systems tab.

The Add Systems page is displayed with several tabs. The first tab allows you to enter a system by entering its information directly. **From List** displays all the systems that are currently in the Cisco TMS database either through discovery or by manual addition. **Pre Register Systems** is for adding systems that may not be online yet. **Add Room/Equipment** adds specialized types of systems used in Cisco TMS Scheduling.

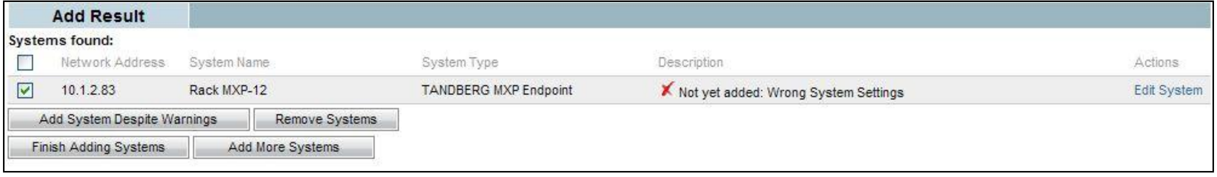
2. In the Add systems page, enter the IP Address or Hostname of the system. Select in the Location Settings. (Multiple systems can be added at once using a range[4] or comma separated list of IP Addresses.)

   The **Advanced Settings** panel allows you to specify additional optional details. Click on the panel menu bar to expand this section. These choices are not needed this example.

3. Click **Next**.
   A progress window is displayed while Cisco TMS connects to the address and determines the type of system being added, and the system configuration. As part of the process, Cisco TMS configures the management settings so that the system can communicate with Cisco TMS.

4. If a password is needed, Cisco TMS prompts you for the system password. Enter the password and click **Next**

   After Cisco TMS has successfully contacted and interrogated the system, a Results page shows the status for each system that it tried to add.



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

[4] Do not enter large ranges of IP Addresses. Due to system discovery and timeouts required, scan time can be several seconds per IP.

Figure 31 The results page shows statuses

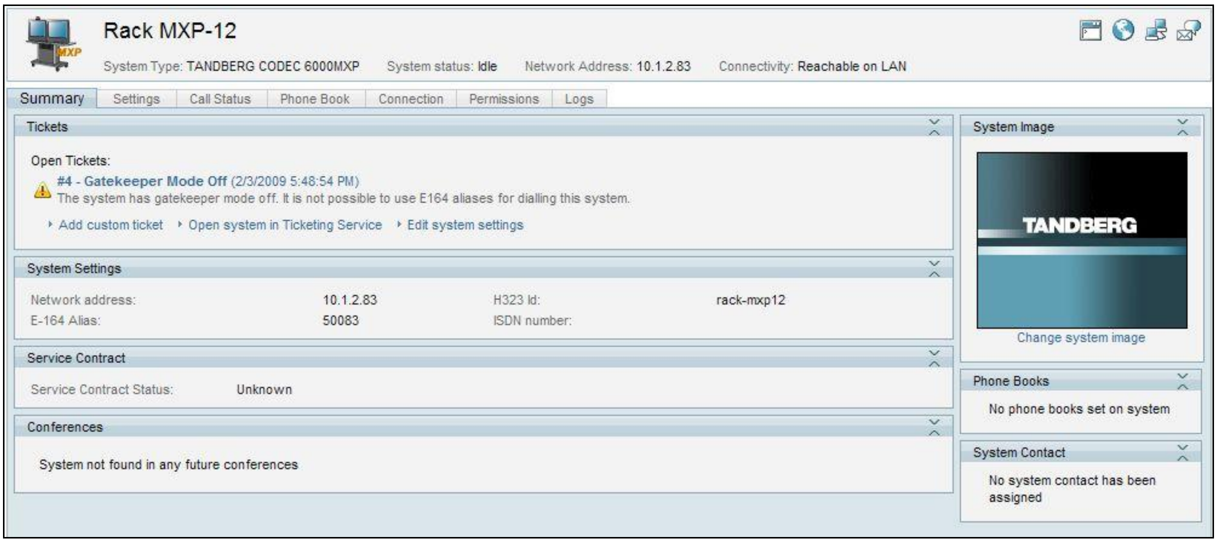
5. If Cisco TMS detected problems with a system configuration, it displays a message in the Description column. You can then edit the system settings by clicking **Edit System**. The settings page for the system describes the error. Edit the settings as necessary and click **Save**. If the problem is resolved, the settings page closes and you are returned to the Add Results page with an updated Description.

   If you do not want to fix the error now, or ignore the messages, clicking **Add System Despite Warnings** in the Settings or Results page adds the system regardless of the existing error condition.

6. Click **Finish Adding Systems** to return to the Navigator with the new system in the folder listing.

Viewing and editing a managed system

A system can be managed from the Cisco TMS interface after it has been added. Navigate to the system in the System Navigator by clicking on its name in the Navigator Tree or by navigating to its folder and clicking on its name in the folder listing in the right panel. The right panel updates to show the system information.



Rack MXP-12

System Type: TANDBERG CODEC 6000MXP System status: Idle Network Address: 10.1.2.83 Connectivity: Reachable on LAN

Tickets

Open Tickets:

#4 - Gatekeeper Mode Off (2/3/2009 5:48:54 PM)
The system has gatekeeper mode off. It is not possible to use E164 aliases for dialling this system.

Add custom ticket · Open system in Ticketing Service · Edit system settings

System Settings

Network address:	10.1.2.83	H323 Id:	rack-mxp12
E-164 Alias:	50083	ISDN number:	

Service Contract

Service Contract Status: Unknown

Conferences

System not found in any future conferences

System Image

Change system image

Phone Books

No phone books set on system

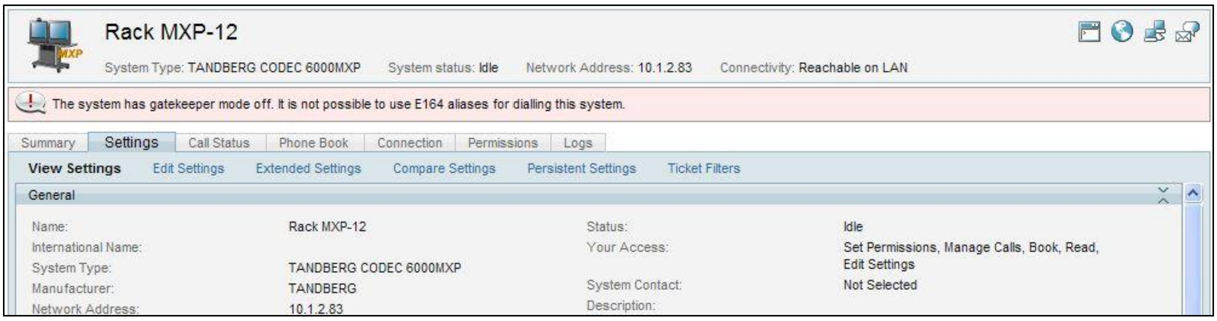
System Contact

No system contact has been assigned

Figure 32 The Summary tab.

The default view is the **Summary** tab which provides an overview of the system and its status.

The **Settings** tab shows a more system configuration detail.



Rack MXP-12

System Type: TANDBERG CODEC 6000MXP System status: Idle Network Address: 10.1.2.83 Connectivity: Reachable on LAN

The system has gatekeeper mode off. It is not possible to use E164 aliases for dialling this system.

General

Name:	Rack MXP-12	Status:	Idle
International Name:		Your Access:	Set Permissions, Manage Calls, Book, Read, Edit Settings
System Type:	TANDBERG CODEC 6000MXP		
Manufacturer:	TANDBERG	System Contact:	Not Selected
Network Address:	10.1.2.83	Description:	

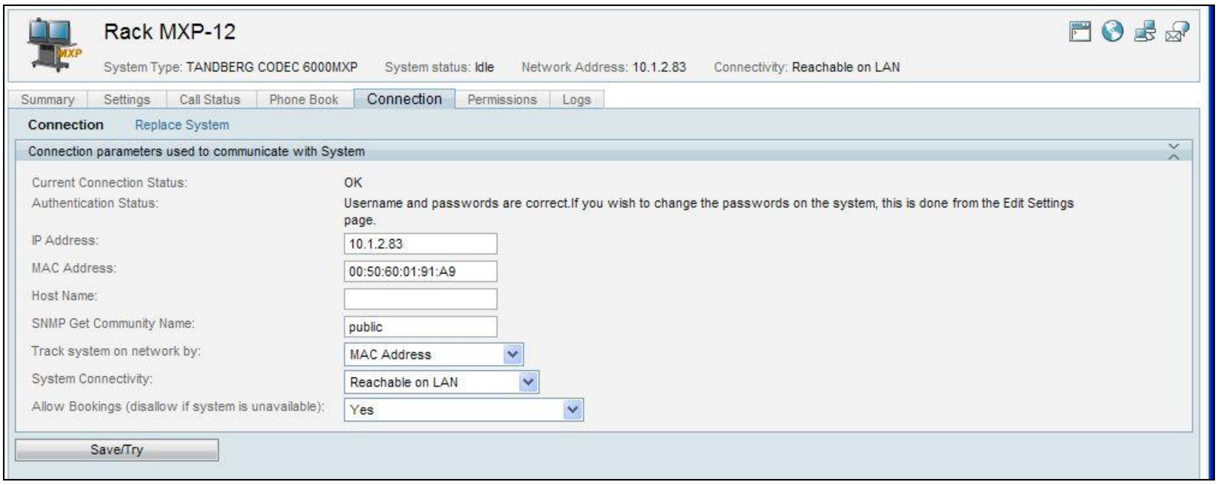
Figure 33 The Settings tab.

You can:

- click **Force Refresh** at the bottom of the page to refresh settings immediately
- click **Edit Settings** in the menu bar to edit any of the settings
- click **Boot** to restart most systems

It is also possible to restart most systems from this screen by clicking the **Boot** button.

If at any time when using these pages, Cisco TMS is unable to communicate with the system, the Connection tab is displayed showing the values that Cisco TMS uses to communicate with the system. Update settings as required and click **Save/Try** to have Cisco TMS try to re-establish communications with the system.



Rack MXP-12

System Type: TANDBERG CODEC 6000MXP System status: Idle Network Address: 10.1.2.83 Connectivity: Reachable on LAN

Connection parameters used to communicate with System

Current Connection Status: OK

Authentication Status: Username and passwords are correct.If you wish to change the passwords on the system, this is done from the Edit Settings page.

IP Address: 10.1.2.83

MAC Address: 00:50:60:01:91:A9

Host Name:

SNMP Get Community Name: public

Track system on network by: MAC Address

System Connectivity: Reachable on LAN

Allow Bookings (disallow if system is unavailable): Yes

Figure 34 The Connection tab.

Update automatically discovered systems

Navigate to the Discovered Systems folder in the System Navigator. View the configuration of each system and update any settings, taking special note of ISDN and IP Zones, as appropriate.

You may also need to update the Permissions for the system so that your new user groups have permission to access the system. Go to the **Permissions** tab.

You can also move the systems to another folder by selecting the check box next to the system and clicking **Move/Copy** when viewing the folder listing.

In the future, Cisco TMS will notify you by email notification whenever it discovers a new system using the System Notification setting that you configured in a previous step. View the newly added system, review and update its settings as necessary.

See the Cisco TMS **Administrator Guide** for more thorough explanations of all the management options available in Cisco TMS.

Configuration templates

Configuration Templates allow you to define a group of configuration parameters as a set to be applied together to systems. The template can even include configuration choices for different system types, and Cisco TMS will only apply the settings that relate to the individual system being updated.

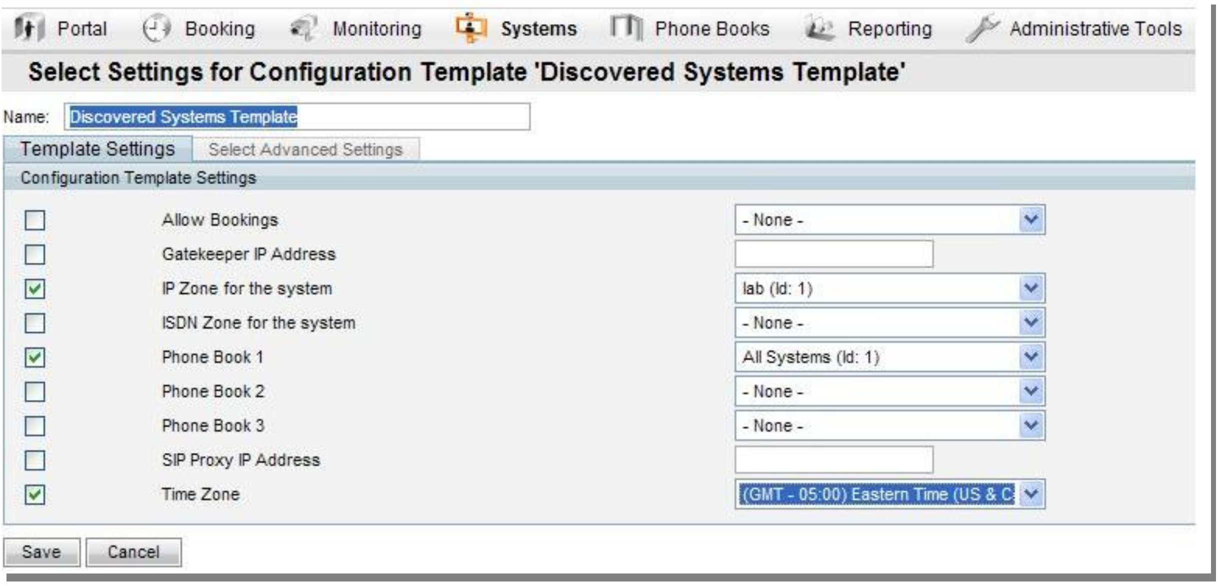
Administrators can define several templates, and can apply them to systems manually, automatically when they are added to Cisco TMS, or even persistently each time the system is powered up. Configuration Templates are managed from the **Systems > Provisioning > Configuration Templates** menu.

As part of the default installation, there is a default ‘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 review this default Template as a working example of how to use Configuration Templates.

Editing a template

1. Open **Systems > Provisioning > Configuration templates**.
2. Click on ‘**Discovered Systems Template**’ to open the **View Settings** page, with all settings and values that make up this template. Note that each item has a setting name, system type, and value. The ‘Type’ for the settings in this template is ‘Other type’ because they are Cisco TMS configuration settings, not configuration options from the device commands itself.

3. Click **Edit** to display the Edit Settings page.



Select Settings for Configuration Template 'Discovered Systems Template'

Name: Discovered Systems Template

Template Settings | Select Advanced Settings

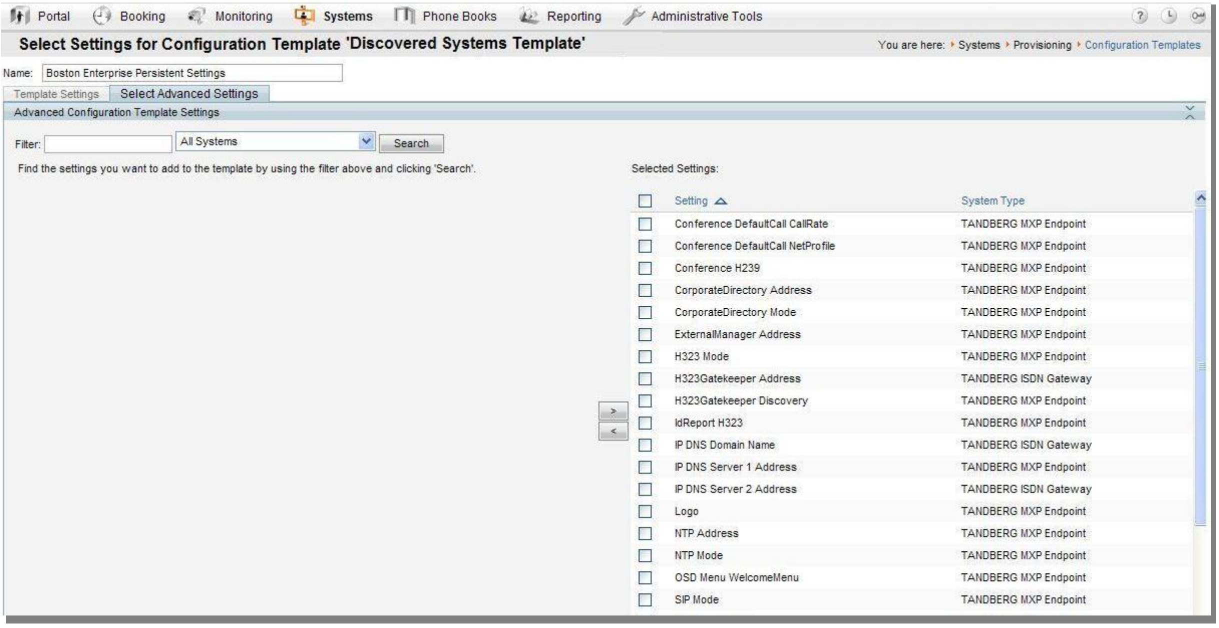
Configuration Template Settings

☐	Allow Bookings	- None -
☐	Gatekeeper IP Address	
☑	IP Zone for the system	lab (Id: 1)
☐	ISDN Zone for the system	- None -
☑	Phone Book 1	All Systems (Id: 1)
☐	Phone Book 2	- None -
☐	Phone Book 3	- None -
☐	SIP Proxy IP Address	
☑	Time Zone	(GMT - 05:00) Eastern Time (US & C

Figure 35 Discovered Systems Template.

4. The **Template Settings** tab opens with all the settings in the templates and their values. Only settings with a selected check box are active in this template. Settings can be enabled or disabled by their check box and values updated using the drop-down lists on the right.

5. All templates have some common Cisco TMS settings initially, such as Zones and Phone books. To add more settings, use the **Select Advanced Settings** tab. From this view, you can chose from all the template settings available in Cisco TMS and add them to the list to be shown in the **Template Settings** tab.



Select Settings for Configuration Template 'Discovered Systems Template'

You are here: ▸ Systems ▸ Provisioning ▸ Configuration Templates

Name: Boston Enterprise Persistent Settings

Template Settings | Select Advanced Settings

Advanced Configuration Template Settings

Filter: All Systems

Find the settings you want to add to the template by using the filter above and clicking 'Search'.

Selected Settings:

☐	Setting	System Type
☐	Conference DefaultCall CallRate	TANDBERG MXP Endpoint
☐	Conference DefaultCall NetProfile	TANDBERG MXP Endpoint
☐	Conference H239	TANDBERG MXP Endpoint
☐	CorporateDirectory Address	TANDBERG MXP Endpoint
☐	CorporateDirectory Mode	TANDBERG MXP Endpoint
☐	ExternalManager Address	TANDBERG MXP Endpoint
☐	H323 Mode	TANDBERG MXP Endpoint
☐	H323Gatekeeper Address	TANDBERG ISDN Gateway
☐	H323Gatekeeper Discovery	TANDBERG MXP Endpoint
☐	IdReport H323	TANDBERG MXP Endpoint
☐	IP DNS Domain Name	TANDBERG ISDN Gateway
☐	IP DNS Server 1 Address	TANDBERG MXP Endpoint
☐	IP DNS Server 2 Address	TANDBERG ISDN Gateway
☐	Logo	TANDBERG MXP Endpoint
☐	NTP Address	TANDBERG MXP Endpoint
☐	NTP Mode	TANDBERG MXP Endpoint
☐	OSD Menu WelcomeMenu	TANDBERG MXP Endpoint
☐	SIP Mode	TANDBERG MXP Endpoint

Figure 36 Select Advanced Settings tab

6. The page has two vertical halves. The list on the right shows all settings that are currently part of the Template. The left panel shows the lists of settings available in Cisco TMS which is empty when you first open the tab. Using the Filter box and Type drop-down, specify what type of setting you are looking for and click **Search**.

7. **Tip:** To see a list of all available settings, leave the Filter blank and the drop-down set to '**All Systems**'.

8. The list populates with all the available settings that match the filter criteria.

9. Add or remove settings by selecting a setting check box and using the < > buttons to add or remove it from the list on the right.
10. Click **Template Settings** to return to the previous tab.
11. Enable or disable individual settings with their check boxes and set the values to use for each setting.
12. When you have finished, click **Save**.

Creating a new template

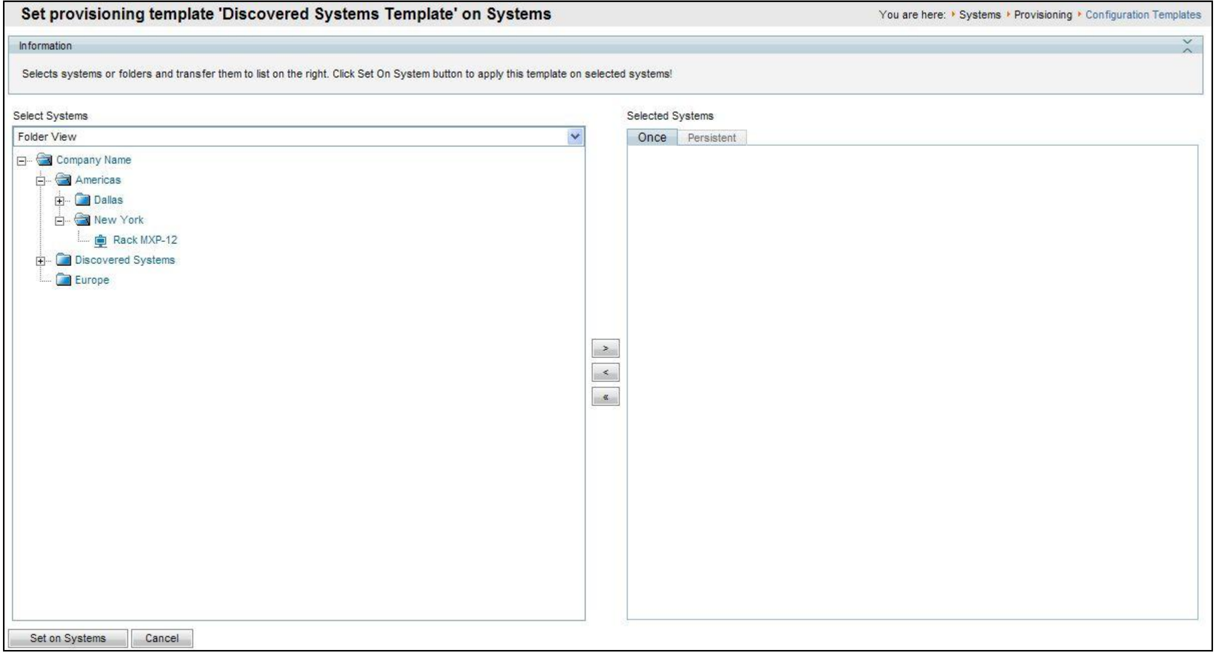
1. To create a new template, go to **Systems > Provisioning > Configuration Templates** and click **New Configuration Template** at the bottom of the Configuration Templates page.
2. Enter a name for the template.
3. Add/remove settings as described in the **Edit Templates** topic.
4. Click **Save**.

Applying templates to systems

An existing Template can be applied to one system or several systems simultaneously. Additionally, Templates can be 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 over the template name you want to use, and click the orange arrow to access the drop-down menu.
3. Click **Set on Systems**.



Set provisioning template 'Discovered Systems Template' on Systems

You are here: Systems › Provisioning › Configuration Templates

Information

Selects systems or folders and transfer them to list on the right. Click Set On System button to apply this template on selected systems!

Figure 37 Set on Systems Page.

4. The Set on Systems page displays two lists: the tree from the System Navigator and a list on the right with two tabs, Once and Persistent. The Once list is all the systems that you will apply this template to. See the TMS Administrator Guide for more information on Persistent Templates.
5. Select a system by clicking on it. Holding the Shift or CTRL keys when clicking to select more than one system. Use the < > buttons to add and remove systems from the Once List.

6. Click **Set on Systems**. The job of applying the template to systems occurs in the background on the Cisco TMS server. You can view the progress in the Provisioning Activity Status page under **Systems > Provisioning**.

Phone books

One of the key features of Cisco TMS is the ability to offer centralized phone books for managed systems. As part of the initial configuration, it is recommended you familiarize yourself with how Phone books are assigned to systems.

There are four main concepts:

- **Phone book** – A listing of contacts. Contacts can include ISDN, IP, SIP, and Telephone numbers for each entry. Multiple phone books can be created in Cisco TMS and each one can be assigned to different users-groups and systems. Phone books are created/managed from **Phone books > Manage Phone books**.
- **Local vs. Server Phone Books** – Local Phone Books are the directories stored and available on most endpoints. These are normally set up and edited from the local endpoint. Server Phone Books are the phone books are created and managed in Cisco TMS, not the endpoint or system.
- **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. Phone book sources are created/managed from **Phone Books > Manage Phone Book Sources.**
- **Setting on 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 multiple phone books for different purposes and assign them to the specific systems that need them. Setting on Systems is done via the Phone book page at **Phonebooks > Manage Phonebooks**. 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** – Utilize ‘TMS User Groups’ to define which user groups are to have read access to each phone book. While, if the Cisco TMS Agent is enabled, utilize ‘Provisioning Directory Groups’ to define which Provisioning Directory Groups shall have access to each phone book.

The default ‘all systems’ phone book

As part of the initial installation, there are two default phone books that are created. The first is a simple phone book that contains all the systems that are managed by Cisco TMS, and this phone book is 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 is from a phone book source that was created during installation.

The second default phone book created during initial installation is the Provisioning Phone Book. If the Cisco TMS Agent is enabled, this phone book contains all the users that are found in the **Provisioning Directory**. 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 being used in the Provisioning Directory, then the Provisioning Phone Book Source will not be populated until users begin to log into their devices.

Scheduled conferencing

With your server in place, and systems added into Cisco TMS, you can now look to add new functionality to your network via automated call launching and control. When scheduling conferences with Cisco TMS users do not need to worry about network protocols, MCUs, or gateways: Cisco TMS handles infrastructure choices and compatibility checking automatically. However advanced users can tune the scheduler and tweak the conference selected methods, as needed.

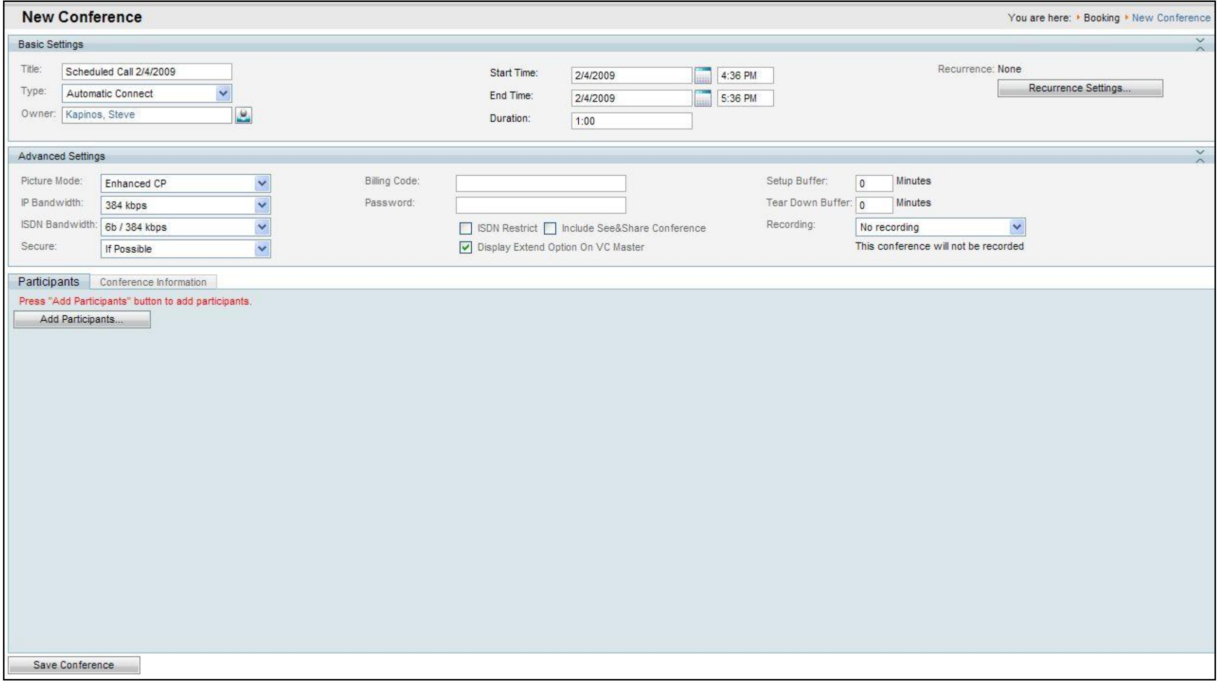
Cisco TMS offers several interfaces to schedule conferences:

- **SCHEDULER** is an interface aimed at the mass audience, with administrator-defined limits on the allowed settings.
- **Free/Busy Overview** is best when you just need to know which systems are available and require a quick meeting.
- The **'New Conference'** page in Cisco TMS is the most robust of all the scheduling interfaces and offers all the possible control and settings.

For this example, we will use the **New Conference** page in Cisco TMS.

Creating your first scheduled call

1. Go to **Booking > New Conference** to open the New Conference page.



New Conference

You are here: Booking New Conference

Basic Settings

Title: Scheduled Call 2/4/2009

Type: Automatic Connect

Owner: Kapinos, Steve

Start Time: 2/4/2009 4:36 PM

End Time: 2/4/2009 5:36 PM

Duration: 1:00

Recurrence: None

Advanced Settings

Picture Mode: Enhanced CP

IP Bandwidth: 384 kbps

ISDN Bandwidth: 6b / 384 kbps

Secure: If Possible

Billing Code:

Password:

□ ISDN Restrict □ Include See&Share Conference

☑ Display Extend Option On VC Master

Setup Buffer: 0 Minutes

Tear Down Buffer: 0 Minutes

Recording: No recording

This conference will not be recorded

Participants | Conference Information

Press "Add Participants" button to add participants.

Figure 38 The New Conference page.

The page has three main areas:

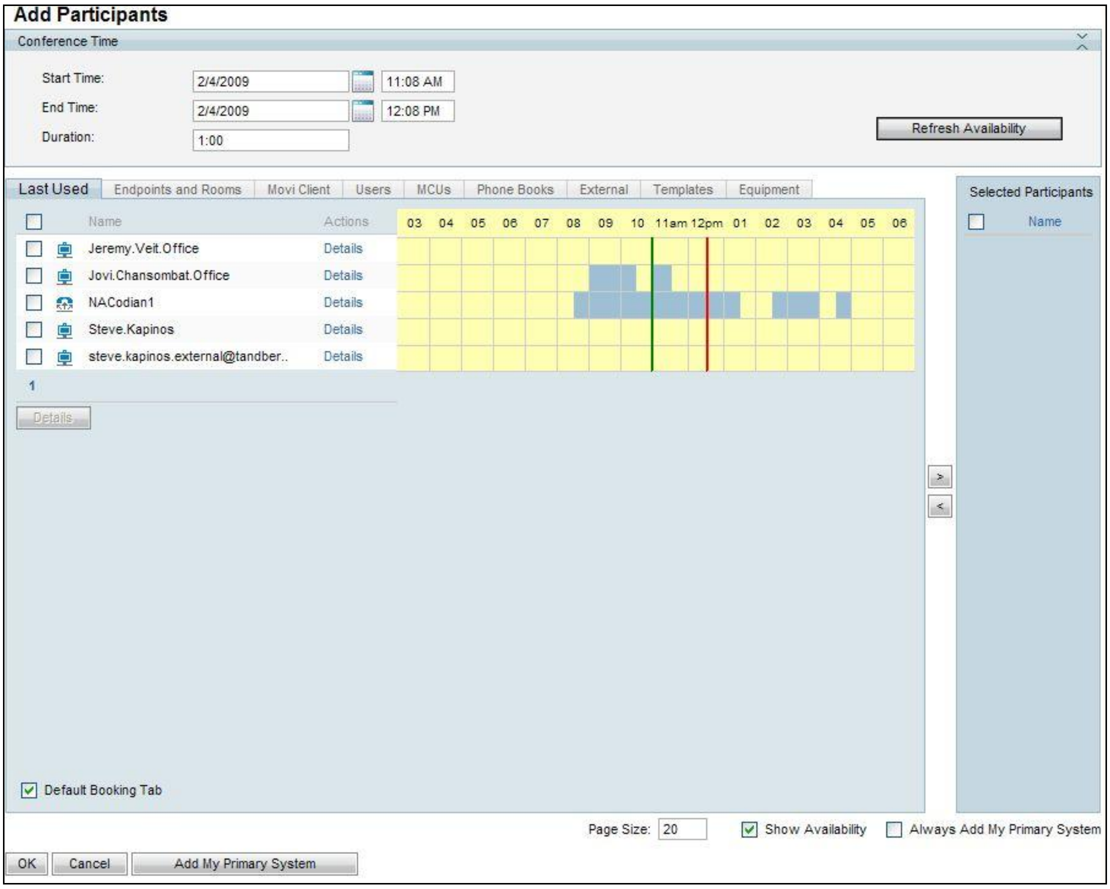
- The top section, **Basic Settings** is primarily for setting the dates and time of the meeting.
- The **Advanced Settings** section in the middle is for setting additional parameters for the conference such as encryption, recording, or bandwidths.
- The bottom section is the most important, where the **meeting participants**, and **call routing information** is presented.

2. Enter a conference Title. This will be displayed in all Cisco TMS interfaces, and is included in the emails sent about the conference.
3. Set the conference start time.
4. Set the duration or end time for the conference.
5. The **Recurrence Settings** button allows you to set a meeting to happen more than oncefor example, a weekly or daily meeting.
   In the **Advanced Settings** section, set the configuration options for this one conference. Most settings will take their default values from the Conference Default values you configured under **Administrative Tools**. We do not cover all the possible options in this example.

- **Picture Mode** controls the layout of the multiple participant conferences. The three choices map to different layouts depending on the MCU being used: Voice Switched means full screen layouts in which one participant is seen at a time; Continuous Presence means multiple participants at a time with equal sized video windows; Enhanced CP means Continuous Presence with unequal sized video windows. This setting can also be changed "on the fly" while monitoring the conference.
- The bandwidth settings control the speeds at which the calls will be placed there are separate settings for ISDN and IP speeds.
- **Secure** controls whether encryption is used during the conference. If you set it to *'yes'*, Cisco TMS ensures that only endpoints that it knows can do encryption will be scheduled for the conference.

  The **Conference Information** tab is an optional area that allows you to add additional notes about the conference that can be referenced later when reviewing scheduled calls.

6. Add participants to the conference in the **Participant** tab. Click **Add Participant** to open a new window.



Start Time: 2/4/2009 11:08 AM

End Time: 2/4/2009 12:08 PM

Duration: 1:00

□	Name	Actions
□	Jeremy.Veit.Office	Details
□	Jovi.Chansombat.Office	Details
□	NACodian1	Details
□	Steve.Kapinos	Details
□	steve.kapinos.external@tandber..	Details

03 04 05 06 07 08 09 10 11am 12pm 01 02 03 04 05 06

1

☑ Default Booking Tab

Page Size: 20 ☑ Show Availability □ Always Add My Primary System

Figure 39 Available participants

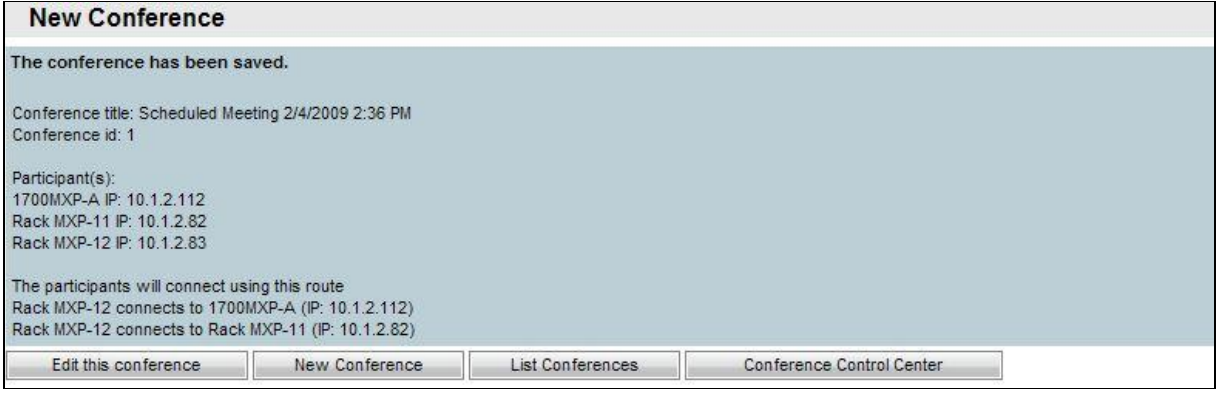
7. Available participants are displayed and a planner view shows their availability, based on existing scheduled and ad-hoc meetings. The colored vertical lines represent your current requested time for the scheduled meeting.
8. The tabs running across the window show all the available types of participants you can select from. If you've used Scheduling before, the default view is a **'Last Used'** tab, giving you quick access to the systems that you have used recently. The other tabs, 'Endpoints and Rooms', MCUs', 'External', and Phone Books, list all the available participants from that category.
   When a category is selected using the tabs, the list of available participants updates showing their availability. Hover over any system, or the blocks in the planner view, for additional details about the system or scheduled meeting.
9. Add participants to the meeting by selecting their check box and clicking the > button to add them to the list of selected participants on the right side of the window.

Note: You do not need to add any network infrastructure components like MCUs, or Gateways; Cisco TMS will handle this for you automatically.

10. To add systems that are not managed systems in TMS, such as dialing to a system in another organization, or adding telephone participants, use the External tab. From here, you can add conference slots for dial in, or dial-out 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 reserves the capacity needed to host the site in the conference and provides you with precise dial-in information to forward to the participant. After all the participants have been added, click **OK**.
11. You are returned to the conference page, with the participant section of the page showing your selected participants. Additional tabs allow advanced scheduling tasks such as altering how calls are connected, or setting specific MCU conference settings for the conference.
12. The Video Conference Master drop-down controls which system is designated the meeting organizer. Cisco TMS will use this system to ask users whether the meeting should be extended when it is about to expire, or that it uses to connect the sites if the conference is not scheduled to be an Automatic Connection. Update the Conference Master, if necessary.

Note: Cisco TMS will only show participants in this list that are compatible with the onscreen messaging features of TMS.

13. Click **Save Conference**. Cisco TMS performs the routing calculations to determine the best way to connect your selected participants. This includes protocol selection, compatibility checking, ensuring systems are available, manipulating ISDN numbers as needed, and including infrastructure resources needed, such as including a MCU or recording device.
    If Cisco TMS is unable to complete your booking request, due to lack of availability, lack of network resources, or there is no known route to connect the participants together, you are returned to the New Conference page and a message banner shows why it was not possible to save the meeting. You can edit the conference settings to try to resolve the issue and save the conference again.
14. If Cisco TMS completes your request, you see a Confirmation page showing the details of your meeting, including the participant list and how each of those participants are scheduled to connect to the conference, including the exact dial string any participants must dial. The Conference ID is a unique identifier for a conference that allows administrators to quickly identify a specific instance of a meeting.



New Conference

The conference has been saved.

Conference title: Scheduled Meeting 2/4/2009 2:36 PM
Conference id: 1

Participant(s):
1700MXP-A IP: 10.1.2.112
Rack MXP-11 IP: 10.1.2.82
Rack MXP-12 IP: 10.1.2.83

The participants will connect using this route
Rack MXP-12 connects to 1700MXP-A (IP: 10.1.2.112)
Rack MXP-12 connects to Rack MXP-11 (IP: 10.1.2.82)

Figure 40 An ICS attachment

You will also get an email confirmation sent to you with an ICS attachment which allows you to insert the event directly into your Outlook (or compatible) calendar.

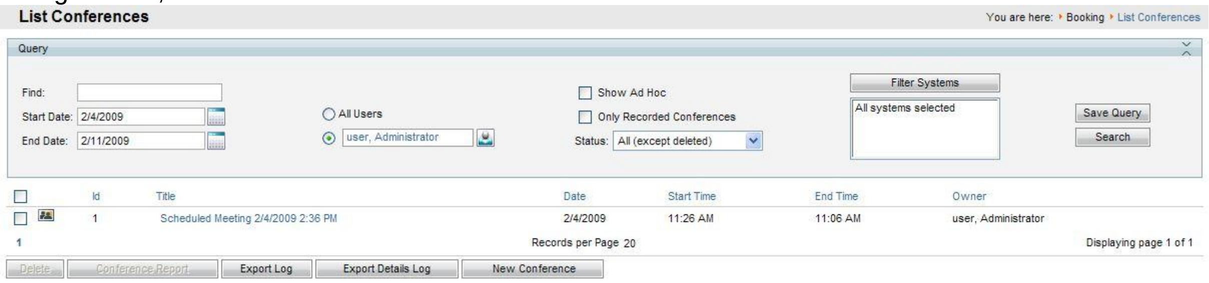
Viewing existing conferences

To find the details about an existing conference, you can use the List Conferences feature. From this view, you can see all the settings that were configured for the conference, the route Cisco TMS built to connect the call, and a log of events. If the conference is scheduled for a time in the future, you can also edit the conference to change its settings.

1. Go to **Booking > List Conferences**.
2. The top portion of the screen allows you to filter the list based on specific criteria such as date, conference owner, status, and even participants. To filter the list, set the parameters you wish and click **Search**.

Note: By default when entering this page, you will only see conferences owned by you. If you wish to see all conferences by all users, select All Users and click **Search.**

3. To view a conference, hover over the title in the list. Open the drop-down menu by clicking the orange arrow, and select **View**.



List Conferences

You are here: Booking ‣ List Conferences

Query

Find:

Start Date: 2/4/2009

End Date: 2/11/2009

○ All Users

● user, Administrator

□ Show Ad Hoc

□ Only Recorded Conferences

Status: All (except deleted)

All systems selected

□		Id	Title	Date	Start Time	End Time	Owner
□		1	Scheduled Meeting 2/4/2009 2:36 PM	2/4/2009	11:26 AM	11:06 AM	user, Administrator

1 Records per Page 20 Displaying page 1 of 1

Figure 41 List Conferences Page.

4. The resulting page looks like the New Conference page, except that you cannot make any changes. Use the tabs in the lower segment of the window to see all the information saved for this conference, including a log of events; the Connection Settings tab shows you how the call was scheduled to connect participants.
   If the conference is scheduled for the future, click **Edit** to modify the conference using the same options that were available to you when creating a new conference. When you save the conference, the previous version is replaced and new scheduling confirmation emails are sent.

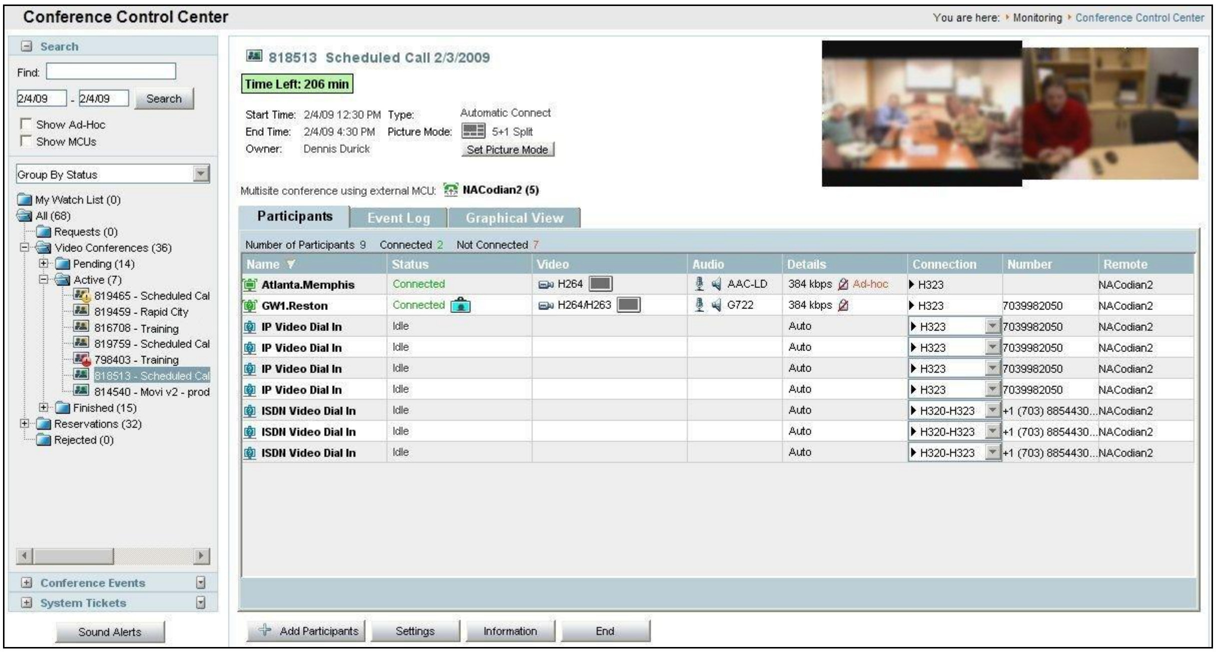
Monitoring and managing ongoing conferences

By monitoring the managed systems on the network, Cisco TMS provides graphical displays and controls of both scheduled conferences (that is, conferences initiated by Cisco TMS) and ad-hoc conferences (those started by users at their own systems).

The most advanced views and controls are available from the Monitoring menu which has three interactive real-time applications.

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 control and interact with the systems in the conference.



Conference Control Center

You are here: Monitoring ▸ Conference Control Center

Search

Find:

2/4/09 - 2/4/09 Search

□ Show Ad-Hoc
□ Show MCUs

Group By Status

- My Watch List (0)
- All (68)
  - Requests (0)
  - Video Conferences (36)
    - Pending (14)
    - Active (7)
      - 819465 - Scheduled Cal
      - 819459 - Rapid City
      - 816708 - Training
      - 819759 - Scheduled Cal
      - 798403 - Training
      - 818513 - Scheduled Cal
      - 814540 - Movi v2 - prod
    - Finished (15)
  - Reservations (32)
  - Rejected (0)

Conference Events

System Tickets

Sound Alerts

818513 Scheduled Call 2/3/2009

Time Left: 206 min

Start Time: 2/4/09 12:30 PM
End Time: 2/4/09 4:30 PM
Owner: Dennis Durick

Type: Automatic Connect
Picture Mode: 5+1 Split

Set Picture Mode

Multisite conference using external MCU: NACodian2 (5)

Participants | Event Log | Graphical View

Number of Participants 9 Connected 2 Not Connected 7

Name	Status	Video	Audio	Details	Connection	Number	Remote
Atlanta.Memphis	Connected	H264	AAC-LD	384 kbps Ad-hoc	H323		NACodian2
GW1.Reston	Connected	H264/H263	G722	384 kbps	H323	7039982050	NACodian2
IP Video Dial In	Idle			Auto	H323	7039982050	NACodian2
IP Video Dial In	Idle			Auto	H323	7039982050	NACodian2
IP Video Dial In	Idle			Auto	H323	7039982050	NACodian2
IP Video Dial In	Idle			Auto	H323	7039982050	NACodian2
ISDN Video Dial In	Idle			Auto	H320-H323	+1 (703) 8854430...	NACodian2
ISDN Video Dial In	Idle			Auto	H320-H323	+1 (703) 8854430...	NACodian2
ISDN Video Dial In	Idle			Auto	H320-H323	+1 (703) 8854430...	NACodian2

Figure 42 The Conference Control Center (CCC)

Graphical monitor

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

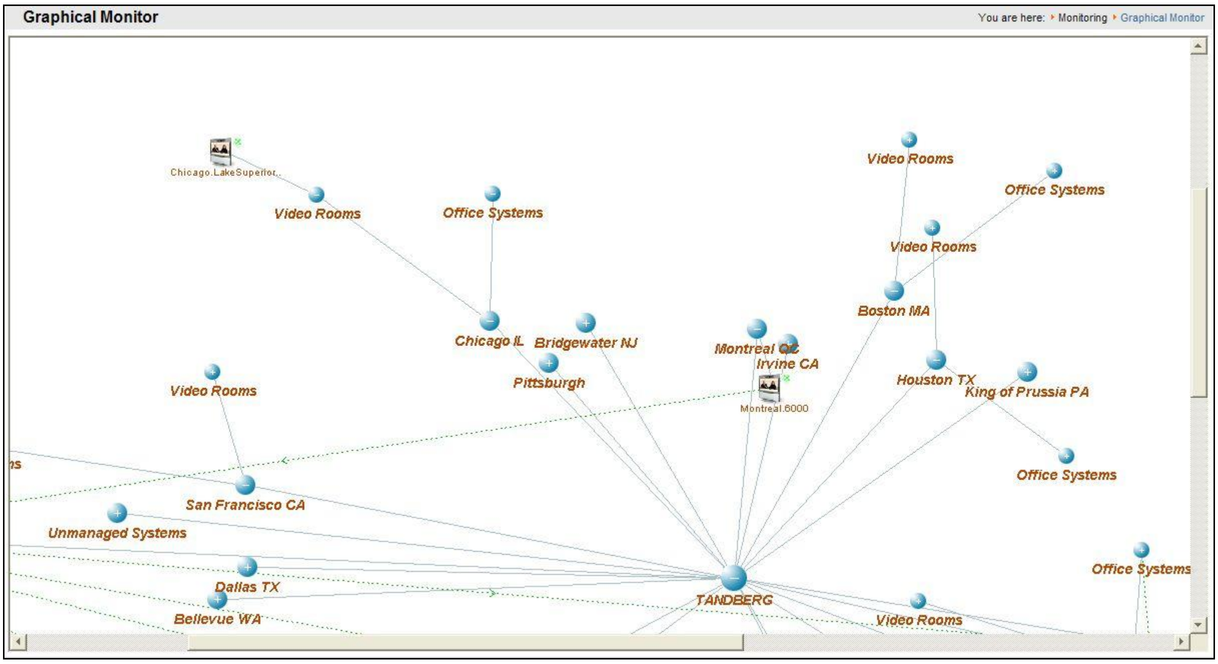


Figure 43 Graphical Map Monitor

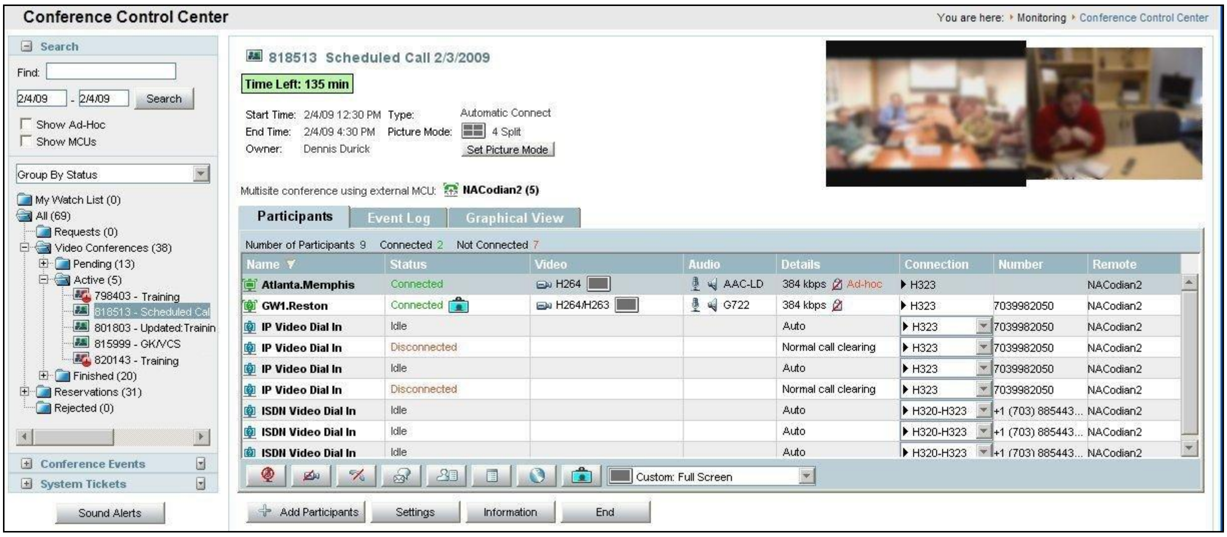
Graphical map monitor

The **Graphical Map Monitor** is a variant of the Graphical Monitor in which, instead of all systems being shown on one page, each folder has its own page and administrators can overlay graphics behind the icons and images; for example, to show geography or system location information.

Monitoring an ongoing scheduled call

Using the **Conference Control Center**, it is possible to get an overview of all ongoing conferences in a single location. CCC has information about upcoming calls, and performs diagnostics on ongoing conferences to alert you (using sound and colored icons) about their status. These diagnostics allow conference operators to monitor large numbers of conferences across the entire network simultaneously without having to manage each device separately.

From the CCC View, the list of conferences is provided on the right, color coded based on their current status. Clicking on a conference in the Details panel on the right.



818513 Scheduled Call 2/3/2009

Time Left: 135 min

Start Time: 2/4/09 12:30 PM
End Time: 2/4/09 4:30 PM
Owner: Dennis Durick
Type: Automatic Connect
Picture Mode: 4 Split
Set Picture Mode

Multisite conference using external MCU: NACodian2 (5)

Number of Participants 9 Connected 2 Not Connected 7

Name	Status	Video	Audio	Details	Connection	Number	Remote
Atlanta.Memphis	Connected	H264	AAC-LD	384 kbps Ad-hoc	H323		NACodian2
GW1.Reston	Connected	H264/H263	G722	384 kbps	H323	7039982050	NACodian2
IP Video Dial In	Idle			Auto	H323	7039982050	NACodian2
IP Video Dial In	Disconnected			Normal call clearing	H323	7039982050	NACodian2
IP Video Dial In	Idle			Auto	H323	7039982050	NACodian2
IP Video Dial In	Disconnected			Normal call clearing	H323	7039982050	NACodian2
ISDN Video Dial In	Idle			Auto	H320-H323	+1 (703) 885443...	NACodian2
ISDN Video Dial In	Idle			Auto	H320-H323	+1 (703) 885443...	NACodian2
ISDN Video Dial In	Idle			Auto	H320-H323	+1 (703) 885443...	NACodian2

Figure 44 The Details panel shows the status, video snapshots, activity logs.

In the Details panel, you can view the status, video snapshots, activity logs from the call, and have full access to interact with the call participants.

The top of the window shows the scheduled time and details of the call. Snapshots, if available, are shown to the top right.

The **Participants** tab allows you to see details of each participant and interact with that call. Each row shows the status, protocols in use, and the call connection details. These views update automatically as you monitor the conference. Clicking on participant name displays icons across the bottom of the list that allows you to disconnect, reconnect, mute, get details about the site, or even change the conference layout the participant is seeing, for example. (Right-click on the participant name to display the same options in a context menu.)

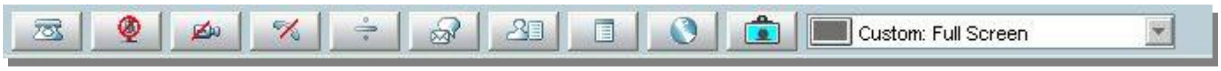


Figure 45 Participant Controls

The **Event Log** tab displays a history log of the conference, showing all connections, status changes, and other details about the selected conference.

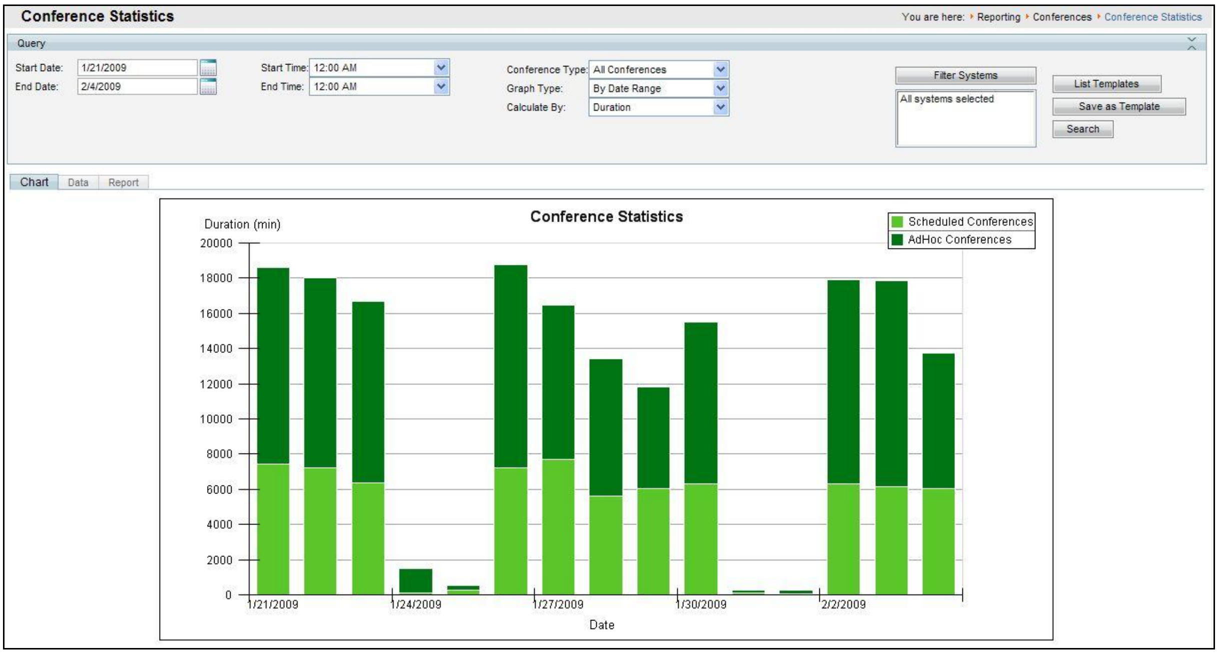
The **Graphical View** tab opens a mini version of the Graphical Call Monitor for just this single conference. At the bottom of the Details window are buttons to interact with the conference as a whole. You can add participants to the ongoing conference, change the conference settings, see any additional information that was entered when the conference was booked, and end the conference.

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 vs. actual usage, and even a ROI Calculator based on actual conferencing usage.

Reports are available from the **Reporting** menu and are categorized to represent. Cisco TMS offers numerous reports and they all use the same basic interface.



Conference Statistics

You are here: ‣ Reporting ‣ Conferences ‣ Conference Statistics

Query

Start Date: 1/21/2009

End Date: 2/4/2009

Start Time: 12:00 AM

End Time: 12:00 AM

Conference Type: All Conferences

Graph Type: By Date Range

Calculate By: Duration

All systems selected

Figure 46 An 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.

Appendix 1 – 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 TMS are removed automatically by the TMS installer. This information is provided for reference.

Note: If replication is currently enabled between Cisco TMS and Cisco VCS, disable replication before uninstalling.

Uninstalling the Cisco TMS Application

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. If you want to completely remove all Cisco TMS information, see Removing all Cisco TMS information from a server.

To remove the Cisco TMS Application:

1. Go to **Start Menu> TANDBERG** and select ‘Uninstall TMS’ or go to Windows Control Panel and use the Add/Remove Programs function.
2. A welcome window explains that the uninstallation script removes Cisco TMS, but the database and database server must be removed separately. Click **Next**.
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

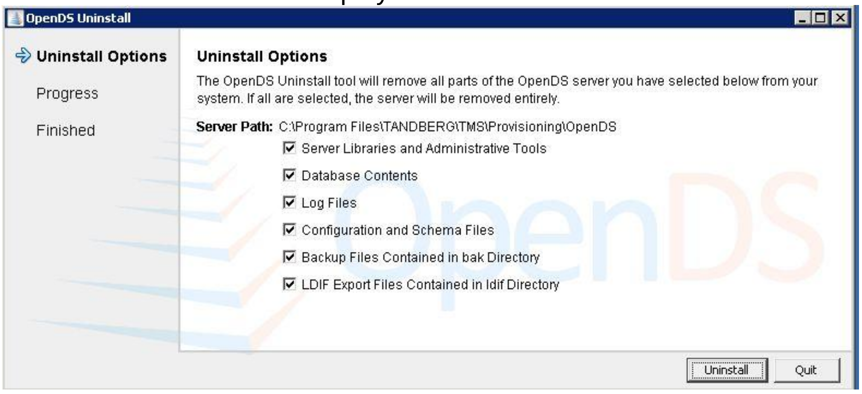
The uninstall wizard only removes the Cisco TMS Application from the server, so that Cisco TMS can easily be reinstalled or upgraded in the future. To completely remove Cisco TMS and all of its data from your server, use the following instructions.

Note: 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 another application.

CAUTION: These steps will delete ALL Cisco TMS data. Do not proceed if you intend to save any information from your Cisco TMS installation.

1. Run the Cisco TMS uninstall wizard using the instructions from Uninstalling the Cisco TMS Application
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:



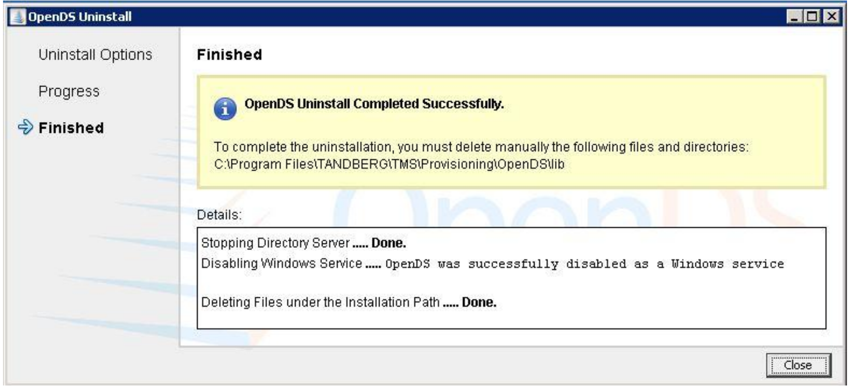
Uninstall Options

The OpenDS Uninstall tool will remove all parts of the OpenDS server you have selected below from your system. If all are selected, the server will be removed entirely.

Server Path: C:\Program Files\TANDBERG\TMS\Provisioning\OpenDS

☑ Server Libraries and Administrative Tools
☑ Database Contents
☑ Log Files
☑ Configuration and Schema Files
☑ Backup Files Contained in bak Directory
☑ LDIF Export Files Contained in ldif Directory

4. Ensure all relevant options are selected, and click **Uninstall**. If you receive a warning stating that the server is currently running, click **Yes** to stop the server.
5. When the database and its files are successfully uninstalled, click **Close**.



Finished

OpenDS Uninstall Completed Successfully.

To complete the uninstallation, you must delete manually the following files and directories:
C:\Program Files\TANDBERG\TMS\Provisioning\OpenDS\lib

Details:

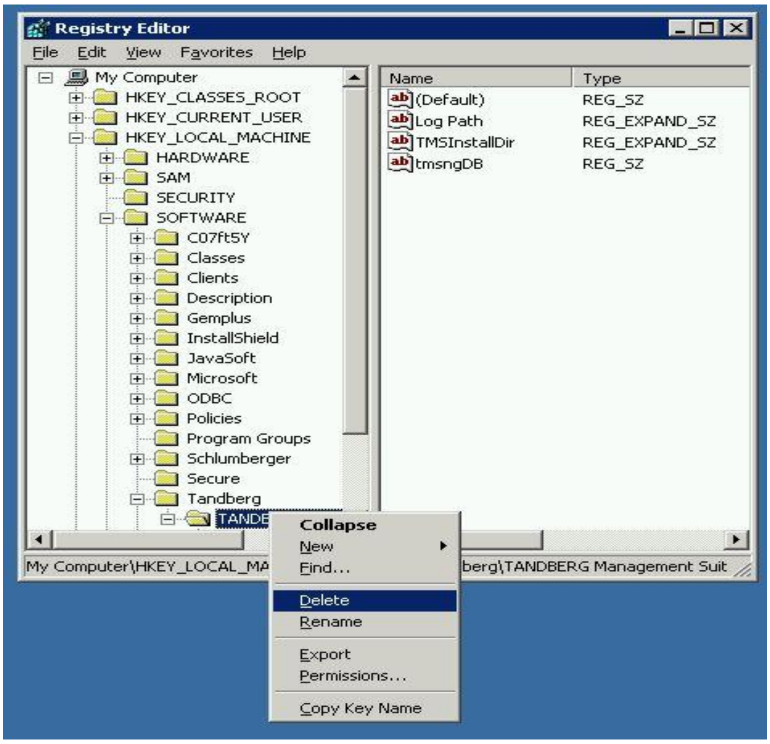
```
Stopping Directory Server ..... Done.
Disabling Windows Service ..... OpenDS was successfully disabled as a Windows service

Deleting Files under the Installation Path ..... Done.
```

Figure 47 The database and its files are successfully uninstalled.

Delete the program folder used by the Cisco TMS installation. The default location is ‘C:\Program Files\TANDBERG\TMS’

6. From the Start menu, select ‘Run...’ and type ‘regedit’ and press return to open the Windows registry editor.
7. Expand the tree on the left using the plus icons to find the Hive (folder) HKEY_LOCAL_MACHINE\SOFTWARE\TANDBERG\Cisco TelePresence Management Suite

8. Right-click on the Cisco TelePresence Management Suite folder icon, and click **Delete**. Click **Yes** to confirm.



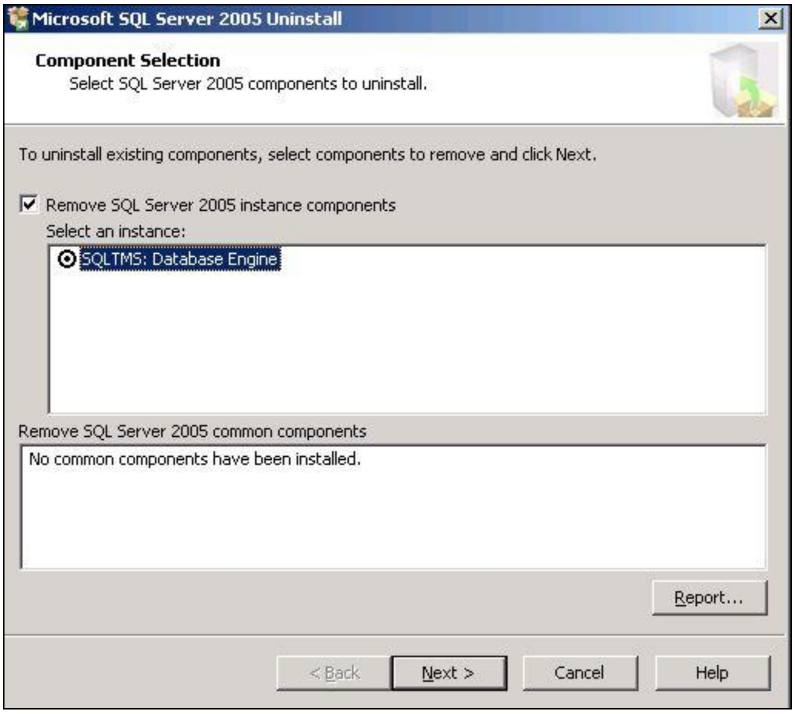
Registry Editor

Name	Type
(Default)	REG_SZ
Log Path	REG_EXPAND_SZ
TMSInstallDir	REG_EXPAND_SZ
tmsngDB	REG_SZ

My Computer\HKEY_LOCAL_MA … berg\TANDBERG Management Suit

Figure 48 Deleting the Cisco TMS Registry Key.

9. Close the registry editor.
10. If you were using a remote SQL Server, ask your SQL Administrator to delete the database named 'TMSng'
11. If the Cisco TMS installer installed a local copy of SQL Server, complete the following steps to remove it:
    a. Go to the Windows Control Panel and open Add/Remove Programs.
    b. Find 'Microsoft SQL Server 2005' in the list and click **Remove**.



Microsoft SQL Server 2005 Uninstall

Component Selection

Select SQL Server 2005 components to uninstall.

To uninstall existing components, select components to remove and click Next.

☑ Remove SQL Server 2005 instance components

Select an instance:

● SQLTMS: Database Engine

Remove SQL Server 2005 common components

No common components have been installed.

    c. Select 'Remove SQL Server 2005 instance components', and 'SQLTMS: Database Engine'.

d. Select Workstation Component from common components. Click **Next**.

e. At the Summary page click **Finish**. The wizard closes automatically when complete.

f. 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.

Checking for updates and getting help

Cisco TelePresence recommends registering your product to automatically receive notifications of the latest software and security updates. If you do not register your product, it is a good idea to regularly check for software updates on the Cisco TelePresence web site. If you experience any difficulties or unexpected results when using this version of the Cisco TMS software, consult the online help for information on using the product.

If the documentation does not answer your question or you have a problem with one of our products, refer to the Support sections of the web site which are kept up to date with the latest information from customer support (www.tandberg.com **> Support**).

If the information on the web site does not help you to solve your problem, contact your reseller. Make sure you have the following information ready:

- the serial number and product model number of the unit
- the software build number which can be found on the product user interface
- your contact email address or telephone number

References and related documents

The following table lists documents and websites referenced in this document.

All Cisco TelePresence documentation can be found on the support website.

For advice from the technical support team on all Cisco TelePresence products, see the Cisco TelePresence knowledge Base.

Name	Document reference
Cisco TMS Database Knowledge Tips	D14216
Cisco TelePresence Management Suite 12.2 Product Support Document	D50546
Cisco TelePresence VCS Deployment Guide - Cluster creation and maintenance (X5)	D14367.3
Cisco TelePresence VCS Software Release Notes (X5)	D50582.3
Cisco TMS v12 Release Notes	D50539.6
Cisco TelePresence Management Suite v11 Release Document	D50418
Cisco TMS Admininstration Guide 13.0	D13741
Cisco TMS 12 Product Support Document	D50546
Online knowledge base	-
Installing licenses; release and options keys for the Cisco TelePresence Management Suite	78-19878-01

Contact us

If you have any questions, comments or suggestions, contact our Online Support service or write to us at:

Product and Sales Support
Cisco TelePresence
P.O. Box 92
1325 Lysaker
Norway

Tel: +47 67 125 125
Fax: +47 67 125 234

Document feedback

This document was written by the Research and Development Department of Cisco TelePresence, Norway. We are committed high quality documentation. Please contact us with comments and suggestions regarding the content and structure of this document.

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