TANDBERG

TANDBERG Management Suite Version 12

Installation and Getting Started Guide

D14389 Revision 01

February 2009

Introduction

Welcome to the TANDBERG Management Server (TMS) Installation and Getting Started document. The TANDBERG Management Suite (TMS) is a portal for carrying out key operations and monitoring your videoconferencing network, supporting TANDBERG and other manufacturers' systems from a central location.

The software suite allows you to book, monitor, maintain, manage and troubleshoot your videoconferencing systems from a single location, ensuring a smooth operation of all systems.

The videoconferencing systems are placed in a structured overview for easy navigation, control and maintenance. The ability to control, monitor, schedule calls and maintain all your videoconferencing systems from one point will dramatically decrease the time used for doing these tasks. TMS integrates into your existing environment, making it easy to make video services available to both administrators and end-users within your organization.

The purpose of this document is to provide you with specific details and information to assist you in the proper installation of the TMS Software Suite or TMS Appliance, as well as providing brief getting started tips with the TMS.

To assist you in this, the document is separated in six sections:

- Section 1 covers the requirements, details and installation instructions to install TMS Software Suite software on a customer supplied dedicated server.
- Section 2 covers additional information needed for customers upgrading from a previous version of TMS. This section **must** be reviewed prior to starting a TMS upgrade to ensure an administrator is aware of any changes required.
- Section 3 covers initial setup, configuration, and operation of the TANDBERG Management Server Appliance. The Management Server Appliance is a hardware and software solution from TANDBERG that comes with the TANDBERG Management Software Suite pre-installed.
- Section 4 provides information and instructions on uninstalling the TMS application
- Section 5 covers device and system support within TMS
- Section 6 covers initial TMS configuration steps that should be performed once TMS has been installed and tips on getting yourself started with TMS.

Further information on TMS and its abilities are available on in the documentation on the TMS installation media (CD-ROM). Additional documentation is provided for specific implementation scenarios such as redundancy and secure setups. TMS also has an integrated online help system to assist you with specific pages and features within TMS. The online help is accessed by clicking the Question Mark icon (?) available on all TMS Pages.

TANDBERG maintains a Frequently Asked Questions (FAQs) and Knowledge Base for TMS on the TANDBERG Website at http://www.tandbergnpd.com/index.htm

TABLE OF CONTENTS

Installing TMS on a Customer Supplied Server

This section will cover the requirements and steps to install the TANDBERG Management Suite on a customer supplied server.

Web Server Requirements

Minimum Hardware Requirements

Pentium compatible processor:	2 GHz or higher
Memory:	1 GB RAM or more. (2GB or more recommended)
Disk Space:	4 GB for installation and Application Footprint (Additional Space required if install SQL Server locally – See Database Server section)

Server OS Requirements

TMS requires a 32bit Windows Operating System. 64bit OSs are not supported at this time. The Server OS must be English, Japanese or Chinese. The following Windows versions are compatible with 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[1] Standard/Enterprise/DataCenter Editions (latest Service Pack recommended)

Dedicated vs. Shared Server:

TANDBERG highly recommends installing TMS on a dedicated server. The level of CPU time and memory usage will vary between installations depending on the activity level and size of the video network being managed. TMS is very resource intensive with specific Server requirements and therefore should not be installed on a server with other Applications or websites are being hosted. TANDBERG will not support installations on shared servers.

TMS may be installed on a Virtual Server, but the TMS virtual machine (child partition) must be provided with sufficient processor resources, memory, and disk resources. TMS's minimum requirements are set assuming TMS has full access to those resources. TMS is known to run properly on VMWare's ESX and Virtual Server products and Microsoft's Virtual Server 2007.

Database Server Requirements

Database Version Compatibility

TMS requires a Microsoft SQL Server 2005 Database Server with Mixed Authentication Mode enabled. All 32bit versions of Microsoft SQL Server 2005 including the Express Edition are compatible with TMS. TANDBERG does not support use of 64bit SQL Server installations at this time.

For customers that do not have an existing SQL 2005 Server, the TMS installer can install Microsoft SQL Server 2005 Express edition locally on the TMS server.

[1] Windows 2008 requires additional configuration steps prior to running the TMS installer. Please see Appendix 1 for further details

Large installations whose database will grow to more than 4GB cannot use Express Edition, and must use a full edition of SQL Server 2005 due to the 4 GB database limitation in Express Edition.

NOTE: MSDE 2000 and Microsoft SQL 2000 are no longer supported in TMS12

> If using an older version of SQL Server, you must upgrade the SQL software **before** upgrading or installing TMS. For assistance upgrading an existing MSDE SQL Server installed by an earlier version of TMS please refer to the TMS Database Knowledge Tips document D1xxxxx which is available on the TMS installation media and on the TANDBERG website.

Database Disk Space Requirements

Database Disk space will depend on size, auditing, and activity level of the video network. In order to control the growth of the database, purge plans for logs and events can be set in the TMS Server Maintenance page (found under Administrative Tools in TMS). Most installations require 1-4 GB for database growth. Ongoing TMS Database information and maintenance tasks are available in TMS under the Administrative Tools menu.

Local vs. Remote Server

The database server TMS is connected to may be installed on the same server as TMS or on a separate SQL server. During installation, you can chose between using an existing SQL Server or having TMS install SQL Server 2005 Express locally on the TMS server.

Using a SQL Server on a separate server has performance benefits due to the high memory and disk I/O load associated with running SQL Server. Running the database server separate from the TMS Server will free up memory and disk resources improving TMS's performance. Running SQL on a separate server is highly recommended for large (100+ system) or high usage video networks.

Database Permissions

When installing or upgrading TMS and using an existing SQL Server, the TMS installer will prompt for a SQL user and password to use. The default is to enter the Server's SA user and it's password. The Server must have Mixed Mode Authentication enabled; Windows Authentication is not supported by the TMS installer.

For new installations, the installer will create a database named 'tmsng' using the SQL Server's defaults. Upgrades will reuse the existing TMS database if found.

If the SA account is not available to use, the following alternatives are available

Automatic Setup, but with security limited role:

> Have your SQL Server administrator create a SQL user and login that has the 'dbcreator' and 'securityadmin' server roles. This account will be the service account for TMS. In the TMS installer when prompted for the SQL Server credentials, enter the created username and password. TMS will create the 'tmsng' database automatically using server defaults and assign itself as owner. TMS will continue to use the supplied account to access the database for ongoing use.

Manual Database creation, max security limited role:

> Have your SQL Server Administrator create a database named 'tmsng' with their desired options. The database collation must be SQL_Latin1_General_Cp1_CI_AS or SQL_Latin1_General_Cp1_CS_AS. Next the SQL Server administrator should create a SQL user and login to use for the TMS Service account and grant the user the 'dbowner' role for the 'tmsng' database. In the TMS installer when prompted for the SQL Server credentials, enter the created username and password. The TMS installer will populate the 'tmsng' database as required and will continue to use the supplied account to access the database for ongoing use.
>
> **NOTE:** The SQL user supplied for TMS to use must always have 'dbowner' permission on the 'tmsng' database, even after installation for TMS to function properly.

Client Software Requirements

TMS is accessed via a web interface for both administrators and users. The following are the software requirements for users to access TMS:

Minimum requirements:

- 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 TMS Server (Local Machine Account or Domain account if server is joined to a domain)

Recommended requirements:

- Microsoft Internet Explorer 7.0 or later
- Mozilla Firefox 2.0 or later
- Java Virtual Machine Runtime Engine (JRE) 1.5.0 or later

A Java Virtual Machine Runtime Engine (JRE) is required for using the Monitoring pages in TMS. If not installed, most browsers will prompt to download and install the browser plug-in automatically from the Internet. If this is not possible due to security restrictions, the JRE may be installed manually on the client computer from the JRE installation file which can be downloaded from http://www.java.com and is included on the TMS installation media for convenience.

Installation Prerequisites

TMS requires specific Server and Network elements for an installation to be completed properly

Required prior to installation

- **Administrator Access to Windows Server and Database** – You must have administrator rights to the Windows Server to complete the installation. If an existing Database Server is to be used, you must have the login information to be used as the TMS Service Account (see **Database Permissions**)
- **.NET 3.5 Framework** – This Microsoft component must be installed before the TMS installation can proceed. The .NET 3.5 Installer can be downloaded from Microsoft and is included on the TMS installation media for convenience.

These component are checked for and installed automatically if not present[2]

- **Internet Information Services (IIS) Web Server**
- **Windows SNMP Services**
- **Microsoft SQL 2005 Server Express Edition (**an existing SQL 2005 Server can also be used**)**

Note: Windows 2008 installations please see Appendix 1 as the IIS installation must be performed manually

Required for TMS operation

- **Domain Membership Preferred** – Each user logging into TMS needs a Windows User Login to authenticate to the website. Users must have either a local account on the TMS Windows Server or a Domain account the server trusts through Active Directory. By making the server a member of the domain, all trusted domain users will automatically be able to use their existing Windows credentials to log into TMS. Limiting what users can do once logged into

[2] Installation of these components may require the Windows Installation CD to complete depending on your type of installation.

TMS is still available through TMS permissions. Active Directory membership is the recommended deployment for most installations as it avoids creating local Windows accounts for each user.

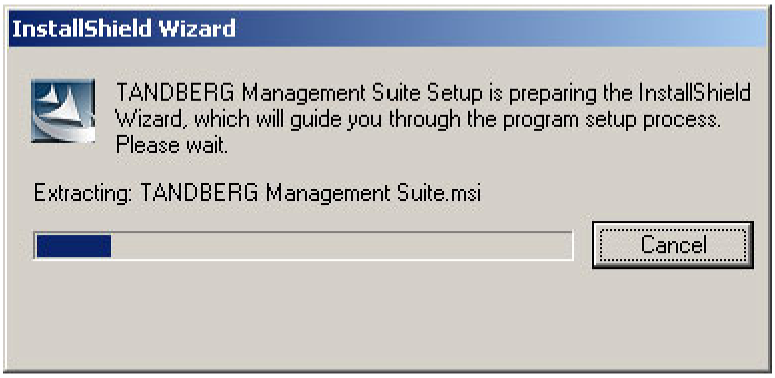
- **ASP.NET and ASP Enabled** – These IIS Components must be enabled. Windows 2008 users please see Appendix 1 for full details on IIS 7 components required
- **TMS Website Accessible by IP and Hostname** - Since not all devices support DNS hostnames or Port Numbers, the TMS website must be accessible by an IP Address on port 80. Some functionality requires TMS to be reachable by hostname so TMS should also be accessible by a fully qualified hostname as well.
- **Mail Server Access** -TMS requires access to a SMTP (Mail) server to be able to send emails out to users. TMS does not require its own SMTP server and can be configured to use your company's existing mail servers. TMS supports SMTP Auth login for authentication if required. If you are unsure which server to point TMS to, please contact your IT Administrator.
- **Network Access to Managed Devices** – TMS needs specific protocols and access to manage devices. Any network Firewalls or NAT routers must allow traffic to flow to and from TMS. The specific protocols and directions in use will vary based on devices being managed. Please see the TMS Product Support document (available on the TMS installation media) for specific on Firewall requirements for each type of supported device.

Note: Many Anti-Virus programs block applications from sending mail directly using the SMTP Port (TCP Port 25). Please verify your Anti-Virus program configuration and verify it will allow programs to send mail using the SMTP Port (TCP Port 25).

Installation or Upgrade of TMS Software Suite

Before you start the installation make sure that you have Administrator user rights and that you have your Windows CD-ROM available (CD may be required for installing some Windows components).

1. Close all open applications and disable virus-scanning software.
2. Ensure that you have installed the Microsoft .NET Framework version 3.5. The installer will check for this before allowing you to complete the installation.
3. Insert the TMS Software Suite CD-ROM into the CD-ROM drive. The Start page on the CD-ROM automatically starts. If CD does not auto start upon being inserted, select Browse.bat in the root directory on the CD-ROM.[3]
4. Click the **TANDBERG Management Suite** software link.
5. You will be prompted to select a Language to use for the TMS Installer. This language will be used only during the installation and does not affect TMS once installed. Select your Language and click 'Next'
6. The TANDBERG installer will prepare the installation wizard.



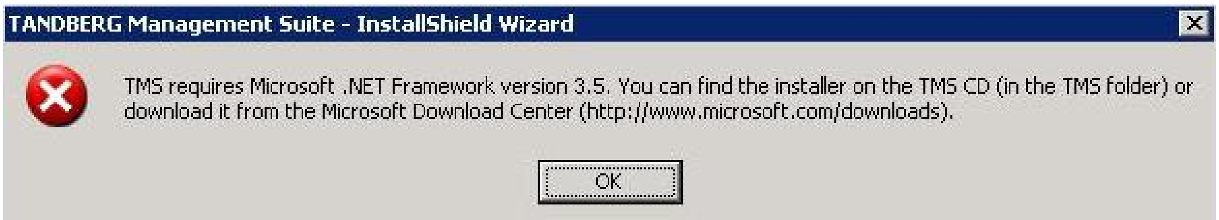
InstallShield Wizard

TANDBERG Management Suite Setup is preparing the InstallShield Wizard, which will guide you through the program setup process. Please wait.

Extracting: TANDBERG Management Suite.msi

[3] If you downloaded TMS as a compressed ZIP file, the ZIP file contents are identical to the CD-ROM's contents. Extract the ZIP to a folder on your computer to access the TMS installation media.

During the preparation, the installer will check if the server has the required software components installed. You may get a warning or error message depending on your server's configuration.

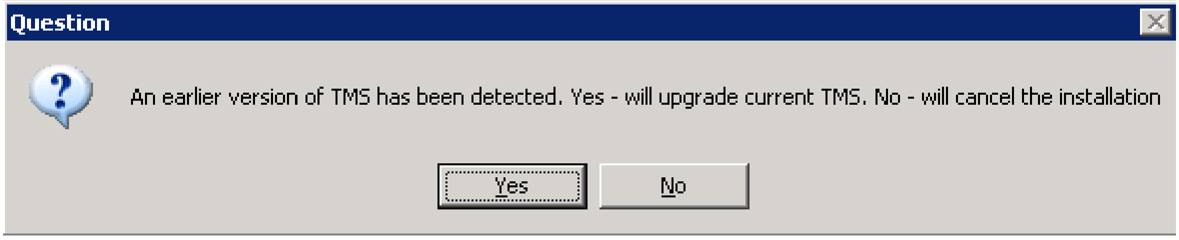


TANDBERG Management Suite - InstallShield Wizard

TMS requires Microsoft .NET Framework version 3.5. You can find the installer on the TMS CD (in the TMS folder) or download it from the Microsoft Download Center (http://www.microsoft.com/downloads).

Example Error Message requiring the Installer be halted

7. The installer will search for a previous installation of TMS. If an earlier version of TMS is currently installed, you will be prompted if you wish to upgrade the existing installation.

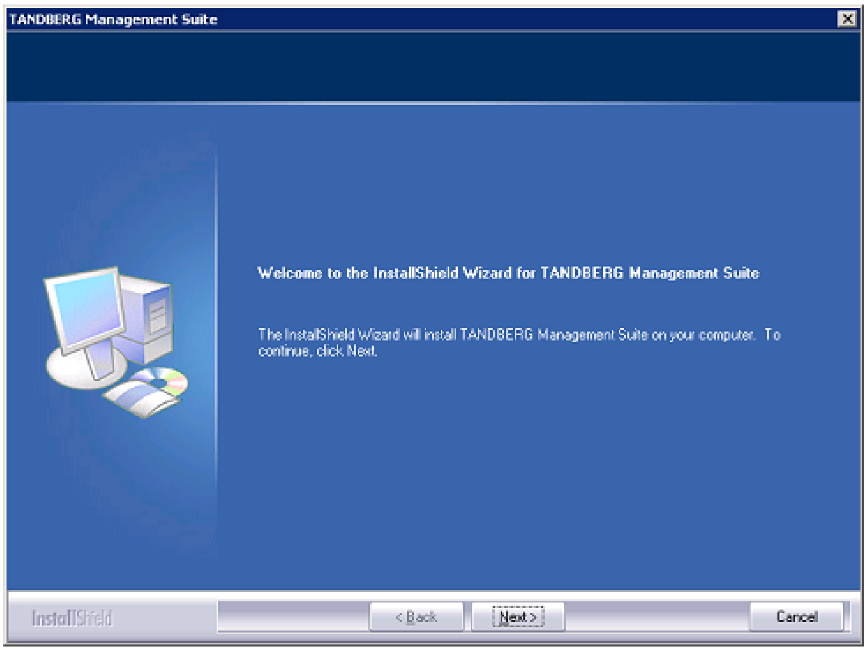


Question

An earlier version of TMS has been detected. Yes - will upgrade current TMS. No - will cancel the installation

Click '**Yes'** to upgrade the current installation. Performing an upgrade will replace the existing version by removing the old version and upgrading the existing TMS database. Clicking 'No' will abort the installation and leave the current installation untouched.

8. A welcome window will appear on the screen. Press the **Next** button to continue. From this point forward you can cancel the installation at any time without further modification to an existing installation or server by clicking the **Cancel** button on any screen before the Summary page.



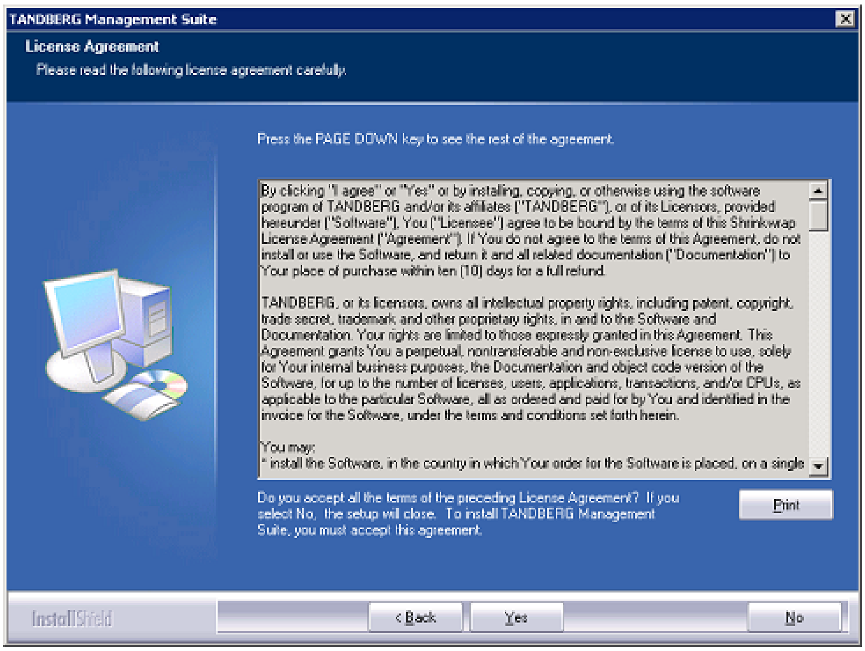
TANDBERG Management Suite

Welcome to the InstallShield Wizard for TANDBERG Management Suite

The InstallShield Wizard will install TANDBERG Management Suite on your computer. To continue, click Next.

Welcome Screen

9. Read through the license agreement and click **Yes** if you accept.



License Agreement

Please read the following license agreement carefully.

Press the PAGE DOWN key to see the rest of the agreement.

By clicking "I agree" or "Yes" or by installing, copying, or otherwise using the software program of TANDBERG and/or its affiliates ("TANDBERG"), or of its Licensors, provided hereunder ("Software"), You ("Licensee") agree to be bound by the terms of this Shrinkwrap License Agreement ("Agreement"). If You do not agree to the terms of this Agreement, do not install or use the Software, and return it and all related documentation ("Documentation") to Your place of purchase within ten (10) days for a full refund.

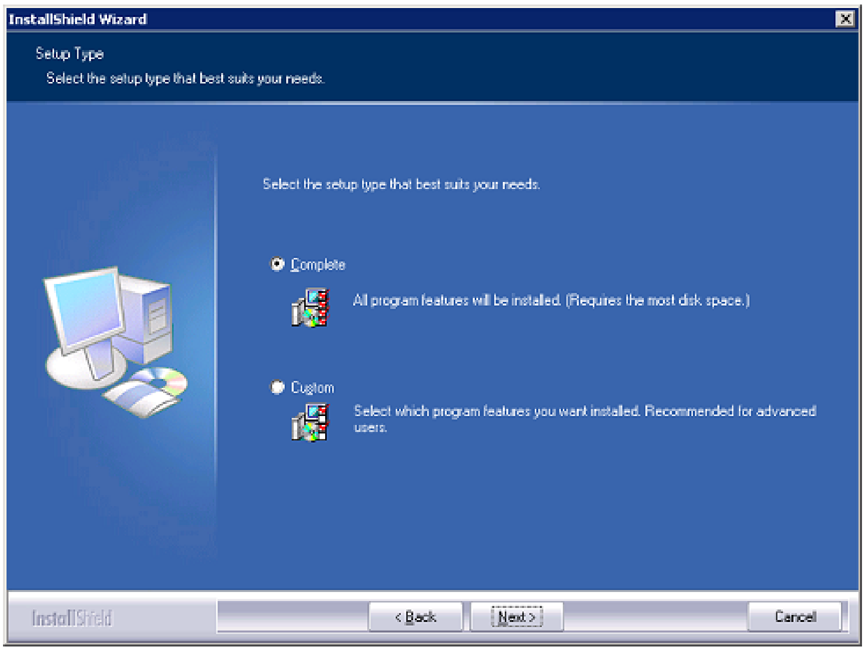
TANDBERG, or its licensors, owns all intellectual property rights, including patent, copyright, trade secret, trademark and other proprietary rights, in and to the Software and Documentation. Your rights are limited to those expressly granted in this Agreement. This Agreement grants You a perpetual, nontransferable and non-exclusive license to use, solely for Your internal business purposes, the Documentation and object code version of the Software, for up to the number of licenses, users, applications, transactions, and/or CPUs, as applicable to the particular Software, all as ordered and paid for by You and identified in the invoice for the Software, under the terms and conditions set forth herein.

You may:
* install the Software, in the country in which Your order for the Software is placed, on a single

Do you accept all the terms of the preceding License Agreement? If you select No, the setup will close. To install TANDBERG Management Suite, you must accept this agreement.

License Agreement

10. Choose Complete or Custom Installation.



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.

Select Installation Type

- 'Complete' Performs the installation using TANDBERG defaults for settings with no extra options such as specifying the installation path or an external SQL Server. 'Complete' can still be used upgrades of existing installations for both local and remote SQL installations and is the recommended choice for performing upgrades.
- 'Custom' option will display all the installation choices available including specifying the installation path and SQL Server choices.

Make your selection and click **Next**. Please jump to **Steps for 'Custom' Installation Choice** if you chose Custom installation.

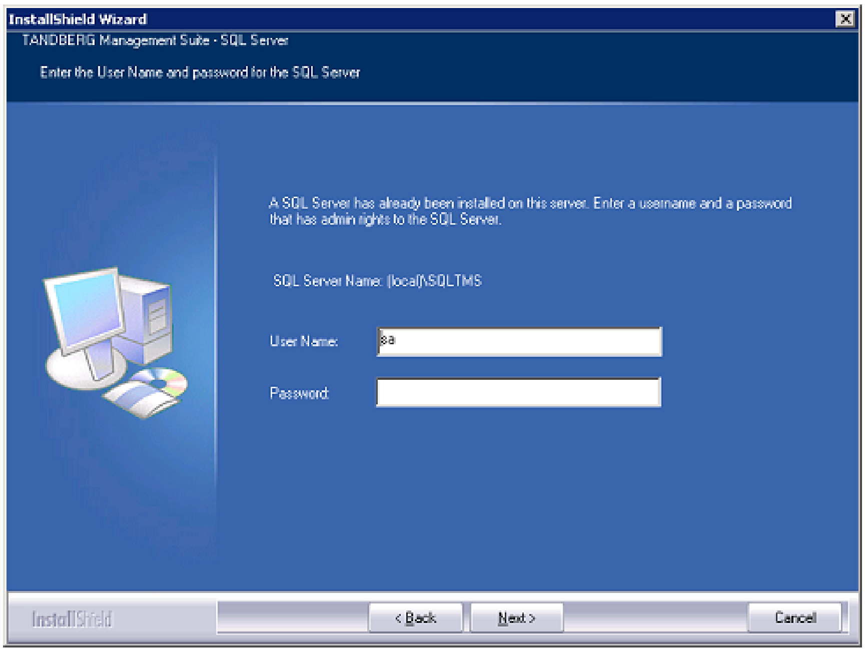
Steps for ‘Complete’ Installation Choice

11. The installer will try to locate an existing SQL Server and TMS database.

    - The installer will look for an existing TMS database connection from earlier TMS installations. If found an existing database connection is found, the SQL Server specified is used. You will be prompted for a username and password to connect to the SQL server. Click **Next** to continue.
    - If no existing TMS database connection is found, the installer will look for a SQL installation on the local server. If found, TMS will prompt for a user name and password to connect to the server so it can create a new TMS database. Click **Next** to continue
    - If no existing TMS database connection or local SQL server is found, the installer will install a local copy of SQL Server 2005 Express Edition and create a new TMS database. The installer will prompt you for a password to set for the SA account (administrator) for the new SQL Server installation. Click **Next** to continue

    NOTE: The SA password must be retained as it is required for future upgrades or TMS maintenance!

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



InstallShield Wizard

TANDBERG Management Suite - SQL Server

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:

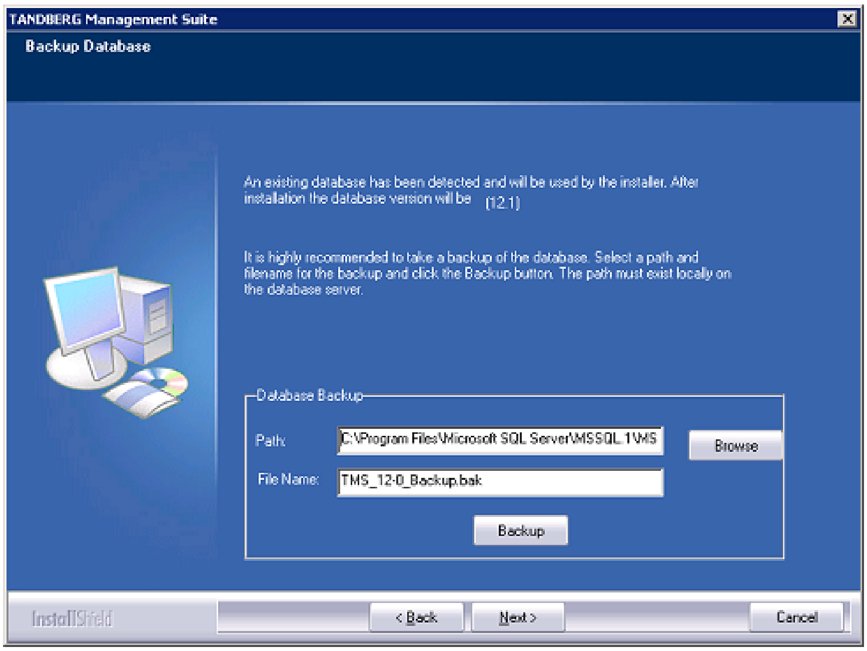
Connecting to an Existing SQL Server

12. If an existing TMS database is found on the SQL server, you will be prompted if you want to re-use the existing database. If the database is an older version and you select ‘Yes’, TMS will automatically update the existing database to the current version and retain the existing information. If you choose ‘No’, the installer will quit and you must manually remove the database from the SQL server if you wish to use that SQL Server. Please ensure you have reviewed **Upgrading From a Previous TMS Version** of this document before proceeding with an upgrade to ensure you are prepared for any additional steps or changes that must be performed based on your previous TMS version.

13. If an existing database is found, the installer will recommend you take a backup of the database before it is upgraded. The backup is optional, but recommended. To skip the backup, simply click **Next**

    To perform the backup, enter a path for the backup file and filename or use the Browse button 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 initiate the backup. You will get a notice when the backup is complete (may take several minutes). When complete, click **Next** to continue the installation.



TANDBERG Management Suite

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.

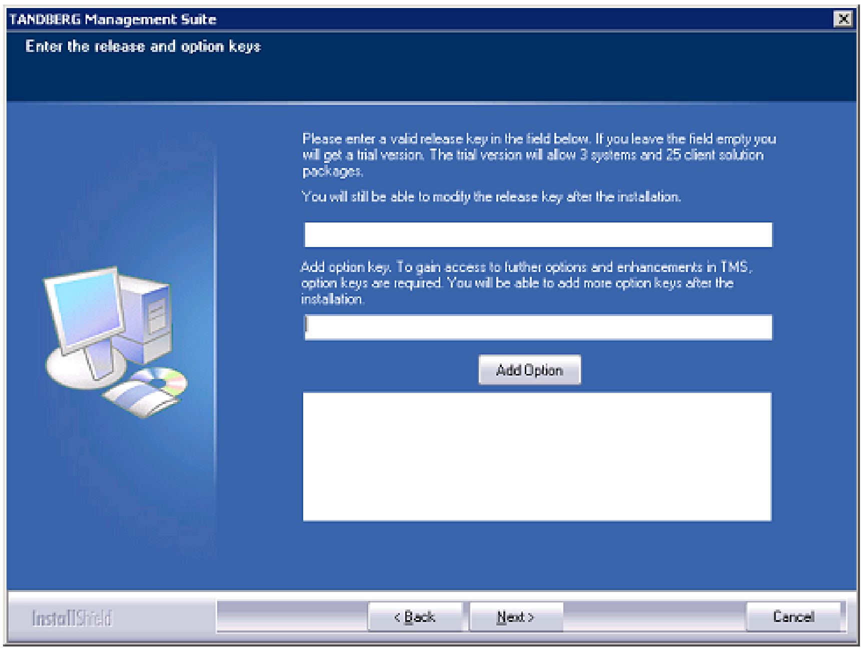
Database Backup

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

File Name: TMS_12-0_Backup.bak

Backup Existing Database

14. The next page allows you to enter your release key and your option keys for enabling additional systems or additional feature support such as Network Integration or other external integration packages. If upgrading from an existing version, your existing keys will be shown. A new release key is required when upgrading to a new major release. For questions regarding your release or option keys, please contact your TANDBERG Reseller or TANDBERG Support.



TANDBERG Management Suite

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.

Enter Release and Option Keys

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

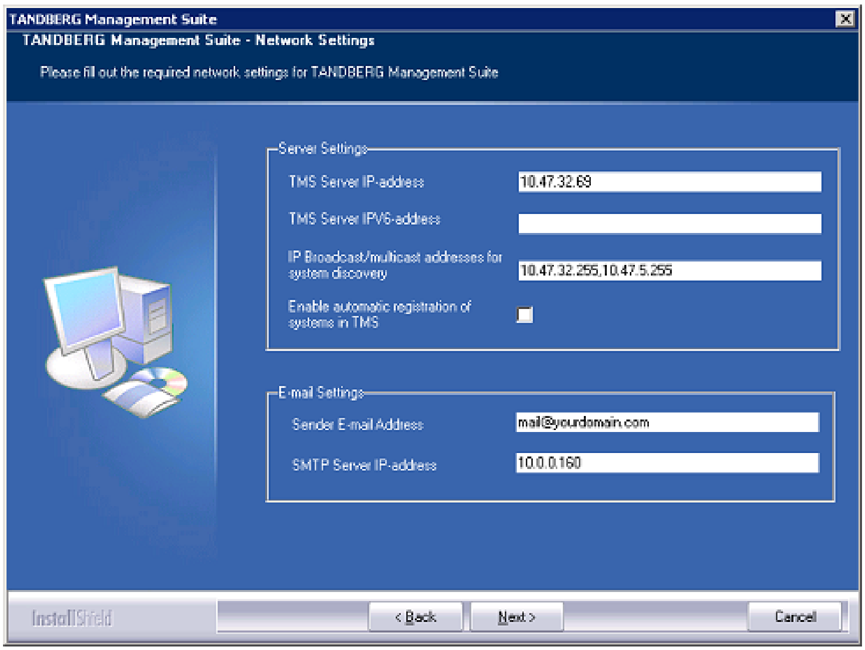
Your release key must be entered before attempting to add Option keys. To add an option key, click the **Add Option** button and enter the key. Keys will be validated before being added to the list. Option keys can also be added post-installation on in the Administrative Tools page in TMS.

Click **Next** when finished entering keys.

The next two screens allow you to pre-configure some default settings to allow TMS to immediately start operating for a basic network configuration. If configured properly, TMS can automatically discover, monitor, log, provide phonebooks, and schedule a basic existing H.323/SIP network. These defaults are to allow a simple network to get up and running quickly and be able to use TMS's main features.

To tune the installation or configure TMS for more advanced networks, you will add further information to TMS and tune these settings in the Getting Started section of this document. All of the settings in the next screens can be further modified once TMS is installed.

15. The Network Settings screen is to configure some essential network defaults to allow TMS to function. If performing an upgrade, the values will be populated with those from the existing database. These settings can also be updated post-installation on the Administrative Tools pages of TMS.



TANDBERG Management Suite

TANDBERG Management Suite - Network Settings

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

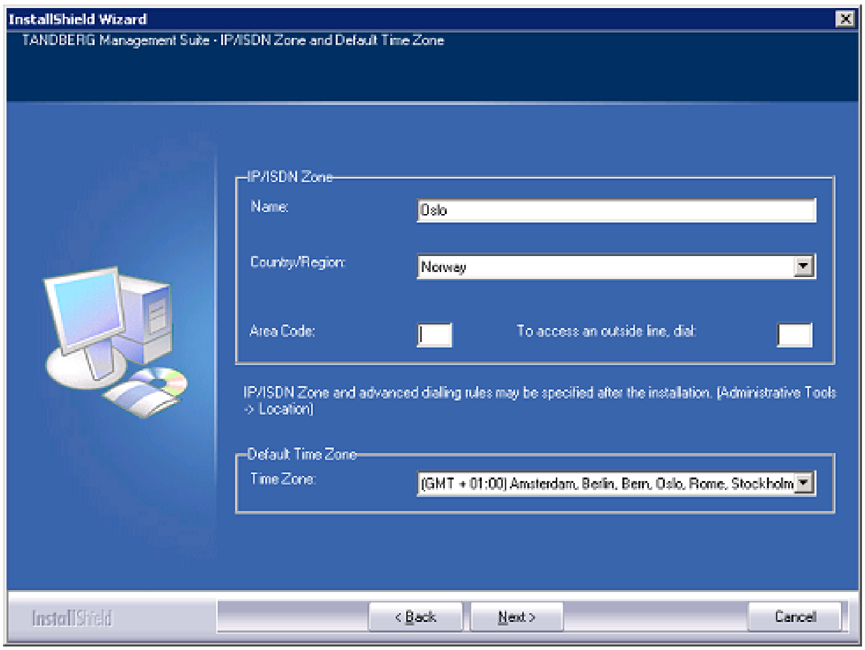
Network Settings

- **TMS Server IP Address** – Verify this is the IP address of the local server. It will be populated automatically if possible.
- **TMS Server IPV6 Address** – Verify this is 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 you wish TMS to automatically search for devices. Systems TMS discovers can be automatically added to TMS with their management settings added. Multiple broadcast addresses can be entered and separated by commas. TMS will search networks by sending a SNMP Discovery packet to the supplied addresses. The default value will be the broadcast address of the TMS server's network.
- **Enable automatic registration of systems in TMS** – If enabled, systems TMS discovers on the network will automatically be added into a folder in TMS and have their management settings configured. The default value is enabled.
- **Sender Email Address** – Enter the mail address you wish to appear as the 'FROM' mail address in emails sent by TMS. Example: videomanagement@company.com

- **SMTP Server IP Address** – Enter the network address of the SMTP server TMS will use to send emails. Additional authentication configuration settings if needed will be setup post-installation.

16. Click **Next**. When leaving this screen, TMS will try to contact the supplied SMTP Server to verify the setting and warn you if it was not able to contact the server.

17. The next screen includes basic defaults for devices and users. Zones are a TMS configuration concept TMS uses to route Phone numbers and aliases when scheduling calls and using Phonebooks. The information entered here will create the first IP Zone and ISDN zone in TMS which will be set as the initial default in TMS. Default zones created here in the installer allow a basic IP network to operate immediately after installing TMS. Additional zones and configurations are added post-installation for networks with multiple locations or more complex elements. The values entered should represent the systems you intend to start with in TMS.


InstallShield Wizard

TANDBERG Management Suite - IP/ISDN Zone and Default Time Zone

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

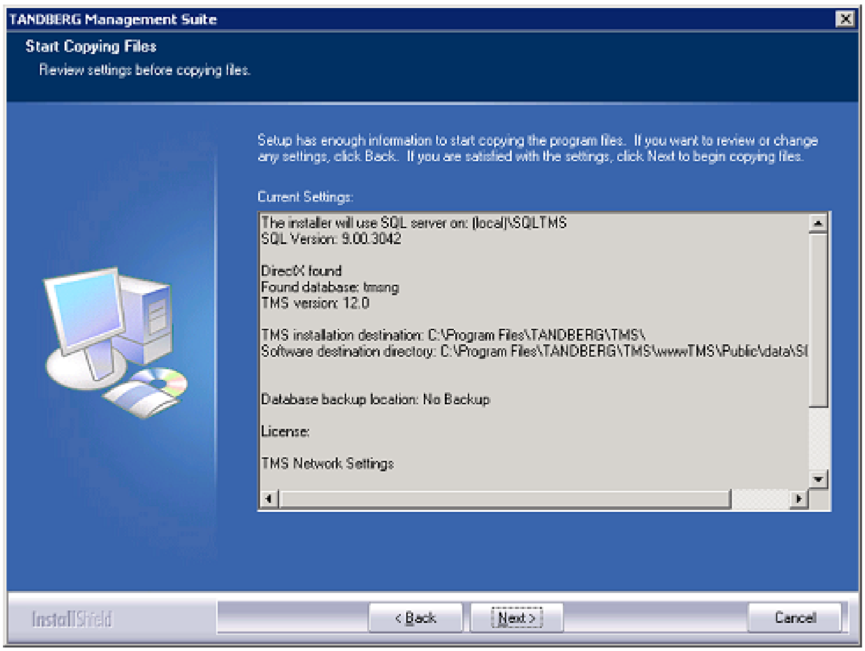
Time Zone: (GMT + 01:00) Amsterdam, Berlin, Bern, Oslo, Rome, Stockholm

Default Zone Information

- **Name** – The name to assign to the zones. Should be descriptive, normally referencing the city or building
- **Country** – Select the Country this zone is located in. This is used for ISDN dialing information
- **Area Code** – Enter the Area Code (if applicable) for the location. This is used for ISDN dialing information
- **To access an outside line [..]** – If you must dial a prefix to reach an outside line on your ISDN circuits, enter it here. This is used for ISDN dialing information.
- **Default Time Zone** – This time zone will be the default used for new systems and users. Chose the most appropriate from the list for your users and systems. Specific settings can be changed later for each user or device.

Click **Next** to proceed once all fields have been completed

18. TMS is now ready to install. A Summary page is displayed with all the settings you have chosen. Verify all settings and click **Next** when ready to proceed.



TANDBERG Management Suite

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\SI


Database backup location: No Backup

License:

TMS Network Settings
```

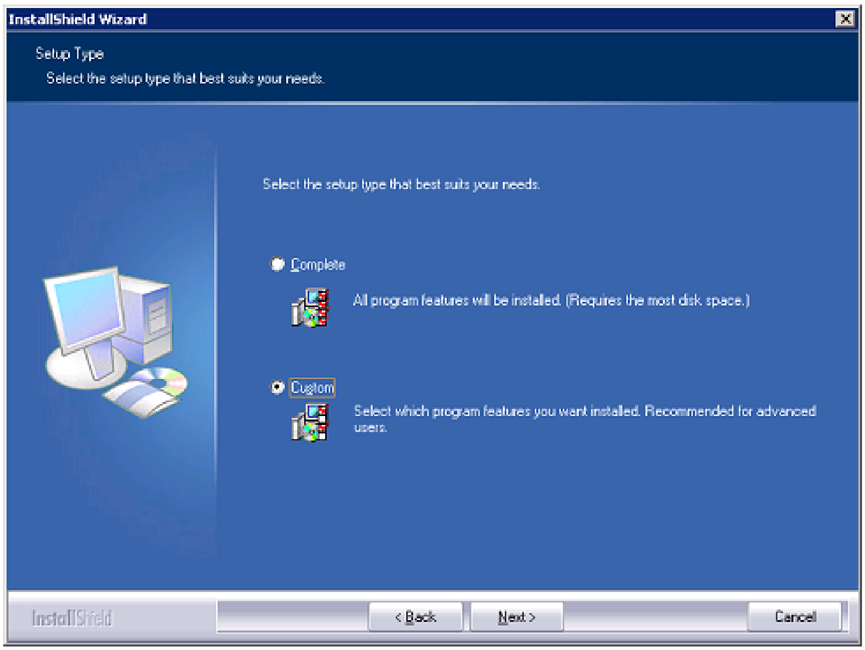
Summary of Settings

NOTE: You may be prompted to reboot the server more than once to complete the installation depending on Windows components that may need to be added. If this is required, the installer will automatically resume after the server reboots.

This completes the installation of the software component of TMS. You should now proceed to Getting Started with TMS to further configure and tune TMS to your individual needs. The remainder of this section covers the steps if the 'Custom' installation option were chosen.

Steps for 'Custom' Installation Choice

Follow the steps 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

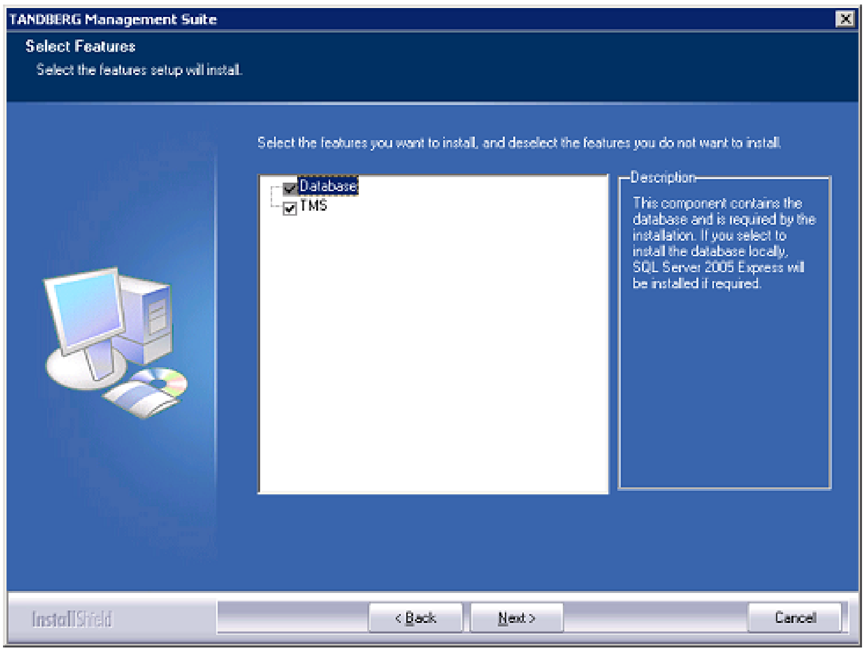
All program features will be installed. (Requires the most disk space.)

● Custom

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

Select Installation Type

1. Choose which components to install. Deselecting TMS will only install SQL Server 2005 Express Edition and the TMS database, if needed. Click **Next** to continue.



TANDBERG Management Suite

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.

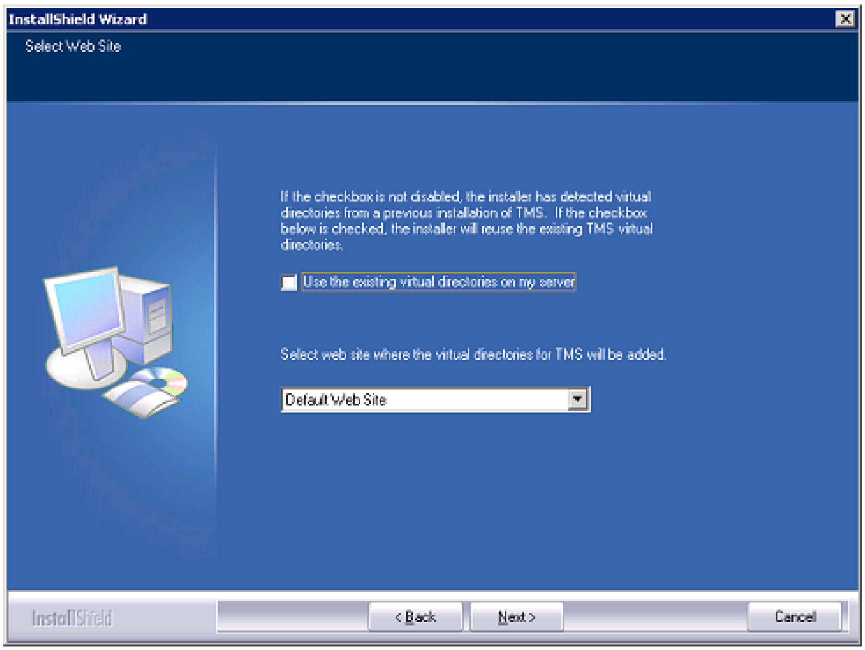
☑ Database
☑ TMS

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.

Select Components to Install

2. Select the Web Site to install into. By Default TMS will install itself by creating a virtual directory in the Default Web Site. If you wish to install TMS into another IIS Web Site besides the Default Web Site, select the Web Site from the drop-down menu.



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

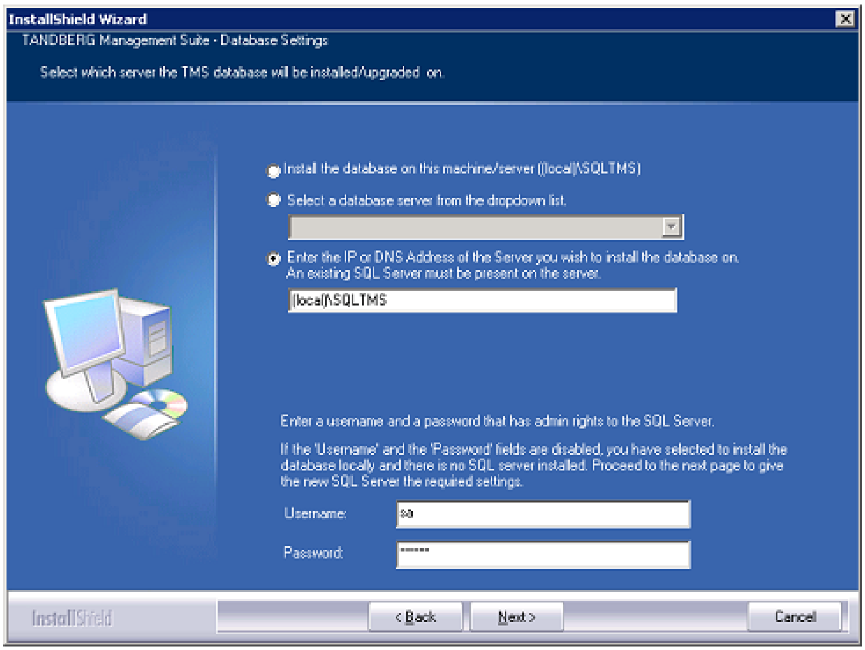
Select IIS Web Site

The installer will detect previous installations of the TMS virtual directories within the IIS server. If you wish to reuse the existing virtual directories, select the checkbox entitled ‘Use the existing virtual directories on my server’ in order to preserve these existing virtual directories. If there are no existing virtual directories used by TMS on the server, the check box enabling you to preserve the virtual directories will be disabled.

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

Make your selections and click **Next**.

3. The next page will allow you to select which SQL server to use. Select from one of the options described below



InstallShield Wizard

TANDBERG Management Suite - Database Settings

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: ******

Select SQL Server Option

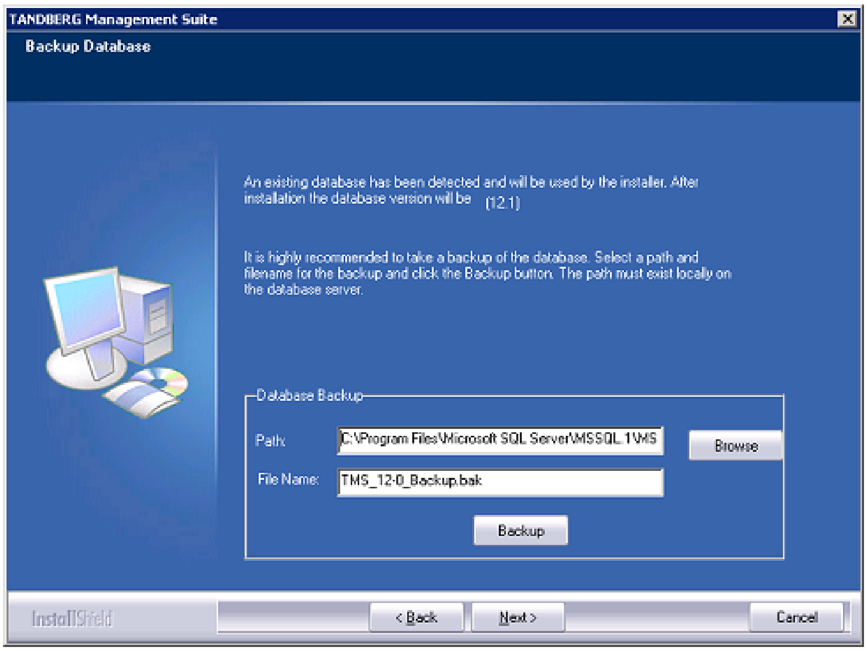
- **Install Database on this machine… (instance name)** – Select this option to install the database on a SQL Server on the local server. If the installer finds an existing SQL install, the name of the instance will be shown in the text and you must supply the SQL Login and password to use at the bottom of the screen. If no local install was found, using this choice installs a new named instance of SQL Server 2005 Express Edition.
- **Select a Database Server from** … - This drop down list will list all SQL Servers the installer was able to locate browsing the network. To install on an existing remote SQL server, select the server from the dropdown list. If you cannot find the server you are looking for, use the next option.
- **Enter the IP or DNS Address of the Server…** - Use this option to install the TMS database on an existing remote SQL Server and the server was not listed in the dropdown. Use the standard Microsoft SQL conventions to specify named instances. Example: **sql1.company.com\vidgrp** If you are unsure of what to enter for your existing SQL server, please see your SQL Server Administrator.

Username/Password – If you selected an existing SQL Server above, enter the SQL Login to access the SQL Server specified. The user specified will be used to create and/or access the TMS database. If you selected to install a new SQL Server locally, these fields will be disabled and a separate page to set a new SA password for the database server will be shown after you click **Next**.

Make your selections and click **Next** to continue.

4. If an existing TMS database is found on the specified SQL server, you will be prompted if you want to re-use the existing database. If the database is an older version and you select 'Yes', TMS will automatically update the existing database to the current version and retain the existing information. If you choose 'No', the installer will quit and you must manually remove the database from the SQL server if you wish to use that SQL Server. Please ensure you have reviewed **Upgrading From a Previous TMS Version** of this document before proceeding with an upgrade to ensure you are prepared for any additional steps or changes that must be performed based on your previous TMS version.
5. If an existing database is found, the installer will recommend you take a backup of the database before it is upgraded. The backup is optional, but recommended. To skip the backup, simply click **Next**

To perform the backup, enter a path for the backup file and filename or use the Browse button 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 initiate the backup. You will get a notice when the backup is complete (may take several minutes). When complete, click **Next** to continue the installation.



TANDBERG Management Suite

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.

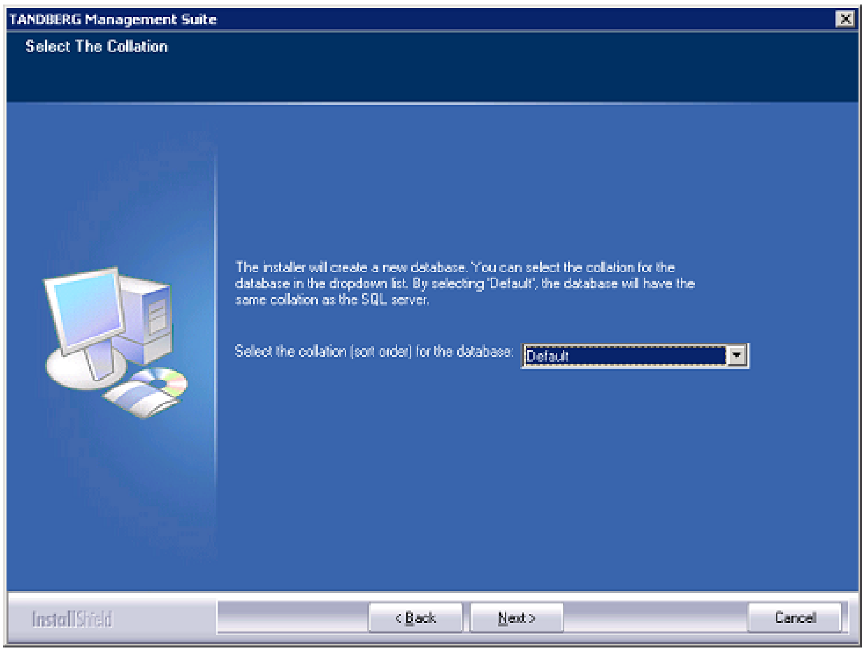
Database Backup

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

File Name: TMS_12-0_Backup.bak

Backup Existing Database

6. If the selected SQL server contains no TMS database, you will be able to select a collation for the new TMS database. By default the collation is the same as the SQL server.



TANDBERG Management Suite

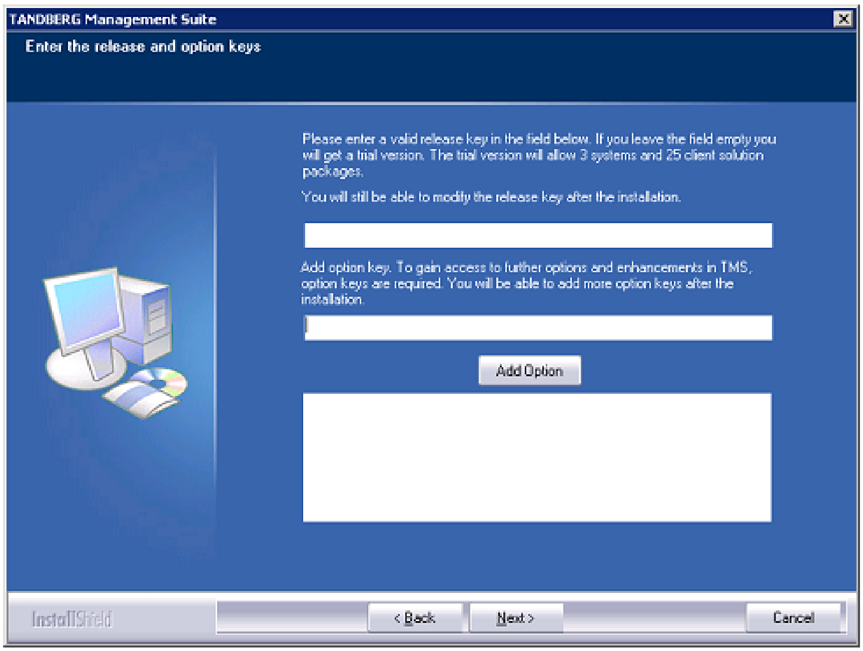
Select The Collation

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

Database Collation

7. The next page allows you to enter your release key and your option keys for enabling additional systems or additional feature support such as Network Integration or other external integration packages. If upgrading from an existing version, your existing keys will be shown. A new release key is required when upgrading to a new major release. For questions regarding your release or option keys, please contact your TANDBERG Reseller or TANDBERG 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.

Enter Release and Option Keys

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

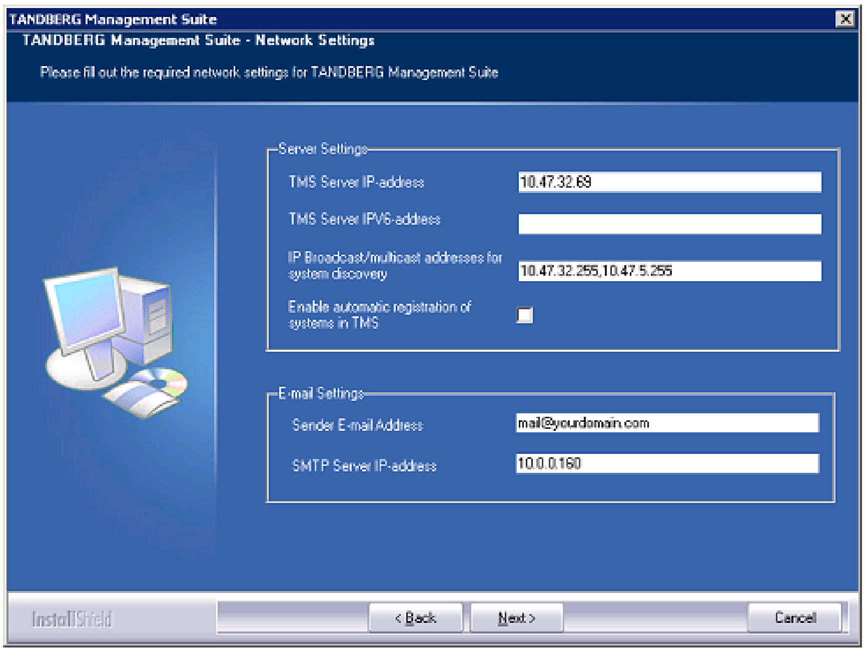
Your release key must be entered before attempting to add Option keys. To add an option key, click the **Add Option** button and enter the key. Keys will be validated before being added to the list. Option keys can also be added post-installation on in the Administrative Tools page in TMS.

Click **Next** when finished entering keys.

The next two screens allow you to pre-configure some default settings to allow TMS to immediately start operating for a basic network configuration. If configured properly, TMS can automatically discover, monitor, log, provide phonebooks, and schedule a basic existing H.323/SIP network. These defaults are to allow a simple network to get up and running quickly and be able to use TMS's main features.

To tune the installation or configure TMS for more advanced networks, you will add further information to TMS in the Getting Started section of this document. All of the settings in the next screens can be further modified once TMS is installed.

8. The Network Settings screen is to configure some essential network defaults to allow TMS to function. If doing an upgrade, the values will be populated with those from the existing database. These settings can also be updated post-installation on the Administrative Tools pages of TMS.



TANDBERG Management Suite

TANDBERG Management Suite - Network Settings

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

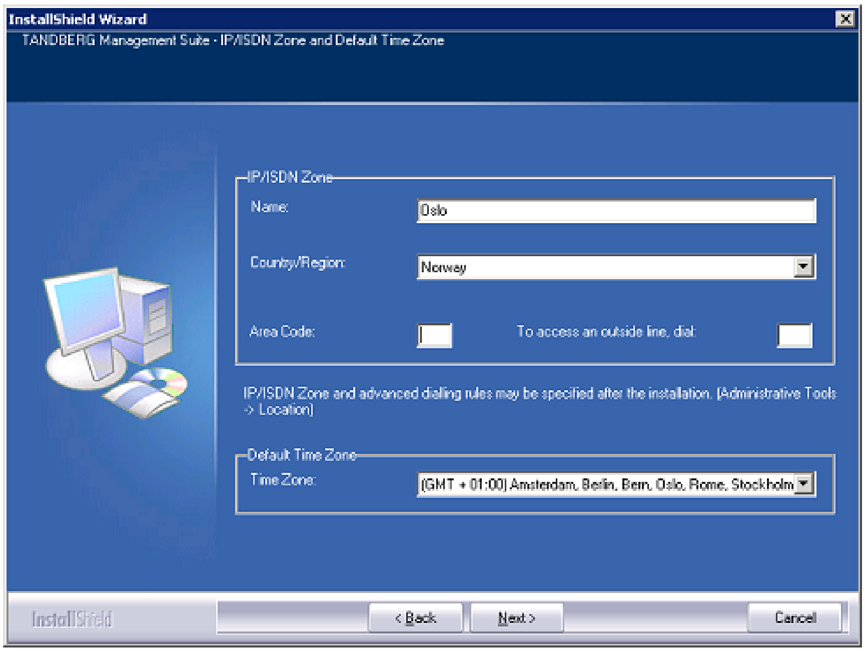
SMTP Server IP-address: 10.0.0.160

Network Settings

- **TMS Server IP Address** – Verify this is the IP address of the local server. It will be populated automatically if possible.
- **TMS Server IPV6 Address** – Verify this is 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 you wish TMS to automatically search for devices. Systems TMS discovers can be automatically added to TMS with their management settings added.. Multiple broadcast addresses can be entered and separated by commas. TMS will search networks by sending a SNMP Discovery packet to the supplied addresses. The default value will be the broadcast address of the TMS server's network.
- **Enable automatic registration of systems in TMS** – If enabled, systems TMS discovers on the network will automatically be added into a folder in TMS and have their management settings configured. The default value is enabled.
- **Sender Email Address** – Enter the mail address you wish to appear as the 'FROM' mail address in emails sent by TMS. Example: videomanagement@company.com
- **SMTP Server IP Address** – Enter the network address of the SMTP server TMS will use to send emails. Additional authentication configuration settings if needed will be setup post-installation.

Click **Next**. When leaving this screen, TMS will try to contact the supplied SMTP Server to verify the setting and warn you if it was not able to contact the server.

9. The next screen includes basic defaults for devices and users. Zones are a TMS configuration concept TMS uses to route Phone numbers and aliases when scheduling calls and using Phonebooks. The information entered here will create the first IP Zone and ISDN zone in TMS which will be set as the initial default in TMS. Default zones created here in the installer allow a basic IP network to operate immediately after installing TMS. Additional zones and configurations are added post-installation for networks with multiple locations or more complex elements. The values entered should represent the systems you intend to start with in TMS.



InstallShield Wizard

TANDBERG Management Suite - IP/ISDN Zone and Default Time Zone

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

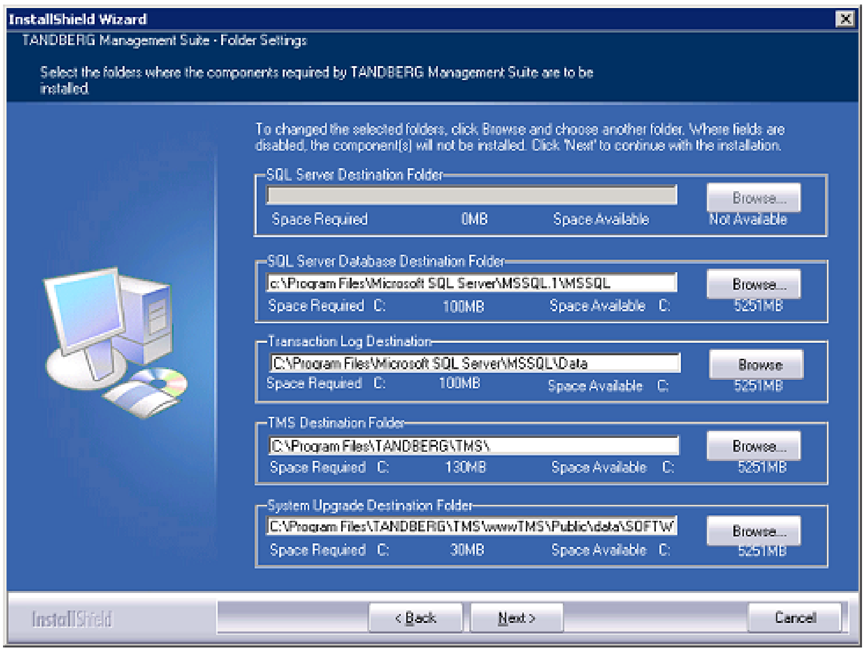
Time Zone: (GMT + 01:00) Amsterdam, Berlin, Bern, Oslo, Rome, Stockholm

Default Zone Information

- **Name** – The name to assign to the zones. Should be descriptive, normally referencing the city or building
- **Country** – Select the Country this zone is located in. This is used for ISDN dialing information
- **Area Code** – Enter the Area Code (if applicable) for the location. This is used for ISDN dialing information
- **To access an outside line [..]** – If you must dial a prefix to reach an outside line on your ISDN circuits, enter it here. This is used for ISDN dialing information.
- **Default Time Zone** – This time zone will be the default used for new systems and users. Chose the most appropriate from the list for your users and systems. Specific settings can be changed later for each user or device.

Click **Next** once all fields have been completed

10. 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 will be grayed out.



TANDBERG Management Suite - Folder Settings

Select the folders where the components required by TANDBERG Management Suite are to be 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

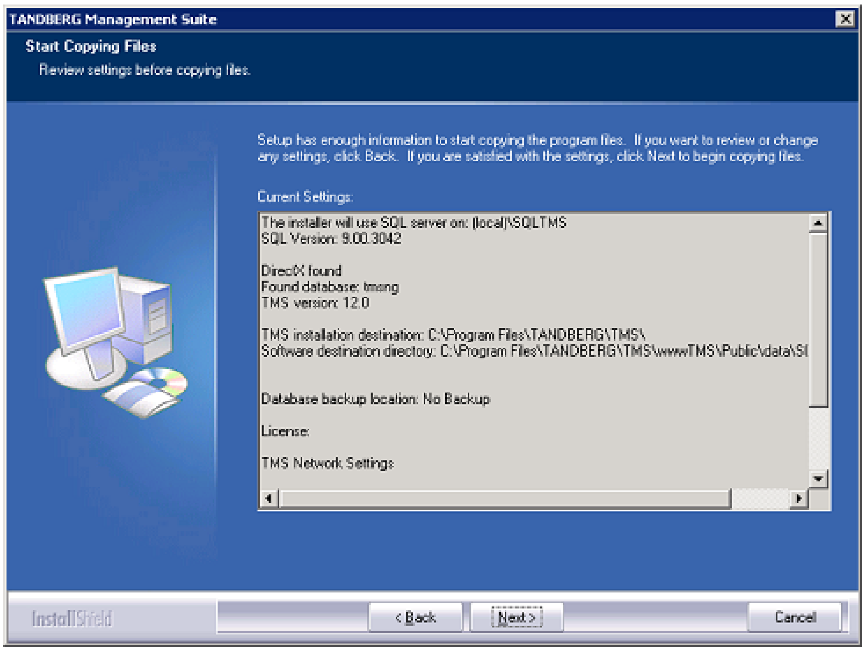
Transaction Log Destination: C:\Program Files\Microsoft SQL Server\MSSQL\Data
Space Required C: 100MB Space Available C: 5251MB

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

Specify Installation Paths

11. TMS is now ready to install. A Summary page is displayed with all the settings you have chosen. Verify all settings and click **Next** when ready to proceed.



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\SI


Database backup location: No Backup

License:

TMS Network Settings
```

Summary of Settings

NOTE: You may be prompted to reboot the server more than once to complete the installation depending on Windows components that may need to be added. If this is required, the installer will automatically resume after the server reboots.

This completes the installation of the software component of TMS. You should now proceed to Getting Started with TMS to further configure and tune TMS to your individual needs. The remainder of this section covers the steps if the 'Custom' installation option were chosen.

Upgrading From a Previous TMS Version

Upgrading of the TMS software itself is handled automatically by the TMS installer. Step by step instructions for running the installer are provided in the previous section of this document, but additional steps may be required to complete the upgrade depending on the previous version used.

Additionally, there may be changes in supported versions or dependencies for other products or integrations that interact with TMS. This section will outline any requirements and additional steps administrators will to consider and complete when performing a TMS version upgrade.

This section is broken into two topics

- Compatibility with Existing Integration Products
- Version Specific Upgrade Notes

Administrators should review this section **before** starting a TMS upgrade to ensure the smoothest upgrade process.

Compatibility with Existing Integration Products

Compatibility with TANDBERG Integration Products for TMS does not change from TMS 12.0 to TMS 12.1. A full list of compatible versions is listed below. **NOTE**: The most recent version may be required to realize all features and fixes.

TMS Integration Compatibility Matrix

Product	Compatible Version
TANDBERG See&Share	v3.3
TANDBERG Microsoft Exchange Integration	All Versions
TANDBERG Microsoft LCS Integration	All Versions
TANDBERG Conferencing eXtensions	All Versions
TMS – IBM Lotus Notes Integration	All Versions
TMS - IBM Lotus Sametime Integration	All Versions
TANDBERG Movi for IBM Lotus Sametime	All Versions
TANDBERG 3rd Party Booking API	All Versions

Version Specific Upgrade Notes

The upgrade process of all previous versions of TMS follows the same principles, but additional steps may be required depending on the version you are currently running. Please be sure to review any version specific notes listed below for the version of TMS you are currently running before starting your TMS upgrade.

Note: Most TMS fixes included for problems related to how scheduled calls are booked do not alter existing conferences. If you are experiencing an issue with a previously booked series of meeting, fixes in your newly upgraded version may not apply to the existing conferences that have yet to execute. This is exaggerated when customers have long series of recurring meetings scheduled from a much older version of TMS. To ensure scheduling fixes are applied to a previously booked series of conferences, open the conference in the List Conferences page. Chose to edit the full series, and click on the Conference Settings page, then save the meeting. This will force the meeting to be updated, ensuring any current fixes are incorporating into the scheduling.

Notes for Upgrades from TMS 12.0

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

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

Customers who were participating in the Movi Beta should refer to their Beta Community Point of Contact for specific upgrade instructions.

Notes for Upgrades from TMS v11.x

The Server requirements for TMS have changed since these TMS versions, including removing support for Windows 2000 Server and Microsoft SQL Server 2000. Please read the **TMS 12.0 Server OS Changes** section for additional details and assistance on upgrading your Server components.

Customers running external integrations must ensure their software is compatible with the new version of TMS or upgrade to the current version. Please see **TMS Integration Compatibility Matrix** for version details.

Customers using TANDBERG Content Servers with TMS, the servers must be running software greater than S2.0. TMS 12.1 is compatible with the most recent Content Server software at the time of this writing which is S3.2. Upgrading from versions prior to S2 require updating the configuration between the servers and updating any future bookings. Additional help to perform these tasks is provided in the Supplement Notes for Manuals section of the TMS v11.6 release in document D50418 TMS v11 Release Notes. TMS Version 11 Release Notes are available from the TANDBERG website.

Starting with TMS v12.0, the permissions were slightly reorganized compared with previous versions. Administrators who implement different user levels through permissions should review their user group permissions after upgrading to TMS v12 and adjust the permissions to their intended settings.

Additional notes for Upgrades from versions 9.x and 10.x

The Server requirements for TMS have changed since these TMS versions, including removing support for Windows 2000 Server and Microsoft SQL Server 2000. Please read the **TMS 12.0 Server OS Changes** section for additional details and assistance on upgrading your Server components.

Customers running external integrations must ensure their software is compatible with the new version of TMS or upgrade to the current version. Please see **TMS Integration Compatibility Matrix** for version details.

TMS has gone through significant changes since these releases and while the TMS installer will import existing data, there are many new settings and existing settings that have changed. Administrators must walk through the Administrative Tools settings in TMS once installed to populate and update TMS's configuration to their environment's needs before considering the upgrade complete. Of particular importance is that the permissions model has been overhauled and Group Permissions and System Permissions should be reviewed and updated to match your needs. Administrators can expect inconsistent behavior between different systems until TMS has refreshed the configuration of each system – normally this will happen automatically within 1-4 hours for most installations.

Additional notes for Upgrade from versions prior to 9.x

For installations older then TMS 9.0, the TMS installer will import your existing data, but TANDBERG recommends a new installation verses performing an upgrade. Server requirements have changed significantly since these versions 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.

TMS 12.0 Server OS Changes

Windows Server 2000 is no Longer supported

Starting with TMS version v12, Microsoft Windows Server 2000 (all versions) is no longer supported as an operating system for the server running TMS. This is due to Microsoft not supporting Windows

Server 2000 in the Microsoft .NET 3.5 Framework and that Mainstream support from Microsoft expired several years ago. Customers running TMS on a Windows Server 2000 OS, must first upgrade their server to Windows Server 2003 before installing TMS v12 or newer. Microsoft recommends performing a clean install when upgrading to Windows 2003 for the best security defaults.

To install on a new server or to allow the existing server to be formatted and have Windows Server 2003 installed, the TMS database should be backed up, along with any customized customer files and stored off the server. Once the server is upgraded, reinstall the original TMS version and restore the TMS database backup. Once your existing TMS installation is up and running, you can proceed to upgrade to TMS v12 or newer. Additional assistance on backing up and restoring TMS can be found in the *TMS Database Knowledge Base Tips* document available on the TMS installation media.

Microsoft SQL Server 2000 No Longer Supported

Starting with TMS v12, SQL Server 2000 (all versions) is no longer supported as a database server for TMS. This change is due to features required for TMS v12 that are not supported in SQL Server 2000 and that SQL 2000 is no longer under Mainstream Support from Microsoft. Customers who are currently running TMS using a SQL 2000 based server (including MSDE 2000 installed by the TMS Installer) must upgrade to a SQL 2005 server before installing TMS v12 or newer. Additional assistance on performing this upgrade is provided in the *TMS Database Knowledge Base Tips* document available from the TMS installation media. Once your existing TMS installation is up and running using a SQL 2005 server, you can proceed to upgrade to TMS v12 or newer.

Customers wishing move the TMS database to a new server, should move the database and or database server prior to running the TMS v12 installer. In order to do this, use the standard Microsoft SQL tools (the TMS database is named 'tmsng'), and then select 'Custom' during the TMS v12 installation. When 'Custom' is selected the user will have the option to specify the database location.

Microsoft .NET Framework 3.5 now required

TMS v12 or newer requires the Microsoft .NET Framework version 3.5 be installed prior to installing TMS. Previous versions of TMS required v2 of the .NET Framework and the .NET version would be installed by the TMS installer automatically if required. Due to the substantially increased size of the new .NET 3.5 installer, the .NET installation is no longer part of the automatic installation process. The TMS Installer will check if .NET 3.5 is installed and if not, stop and prompt the user to install .NET 3.5 before retrying the TMS installation. The .NET 3.5 installer is provided on the TMS installation media and is a simple, automated install. TMS Appliance Users please see **The TANDBERG Management Server Appliance** section of this document for an important step required to complete the .NET 3.5 installation.

The TANDBERG Management Server Appliance

The TANDBERG Management Server Appliance is TANDBERG provided server hardware that comes with the TANDBERG Management Software Suite pre-installed. This combination allows administrators to deploy TMS without the burden of procuring, configuring, or installing their own server and operating system. The TANDBERG Management Server is intended for use by small to medium sized networks (up to 100 managed systems) and includes all necessary software pre-installed to operate.

This section includes four topics

- **Pre-Installation Considerations for Management Server**
- **First time setup and configuration of the TANDBERG Management Server**
- **Operation, Maintenance, and upgrading the TANDBERG Management Server**
- **TMS Software Installation/Upgrades on the TANDBERG Management Server**

For information regarding the configuration of the TMS application itself, please see **Getting Started with TMS** of this manual as well as the *TMS Administrator Guide* for further information.

Pre-Installation Considerations for Management Server

Client Software Requirements

The Management server is accessed via a web interface for both administrators and users. The following are the software requirements for users to access the TMS application:

Minimum requirements:

- 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 TMS Server (Local Machine Account or Domain account if server is joined to a domain)

Recommended requirements:

- Microsoft Internet Explorer 7.0 or later
- Mozilla Firefox 2.0 or later
- Java Virtual Machine Runtime Engine (JRE) 1.5.0 or later

A Java Virtual Machine Runtime Engine (JRE) is required for using the Monitoring pages in TMS. If not installed, most browsers will prompt to download and install the browser plug-in automatically from the Internet. If this is not possible due to security restrictions, the JRE may be installed manually on the client computer from the JRE installation file which can be downloaded from http://www.java.com and is included on the TMS installation media for convenience.

Server Network Requirements

While the Management Server is a self-contained server, it has some network dependencies that must be considered

- **Domain Membership Preferred** – Each user logging into TMS needs a Windows User Login to authenticate to the website. Users must have either a local account on the TMS Windows Server or a Domain account the server trusts through Active Directory. By making the server a member of the domain, all trusted domain users will automatically be able to use their existing Windows credentials to log into TMS. Limiting what users can do once logged into TMS is still available through TMS permissions. Active Directory membership is the recommended deployment for most installations as it avoids creating local Windows accounts for each user.

- **TMS Website Accessible by IP and Hostname** - Since not all devices support DNS hostnames or Port Numbers, the TMS website must be accessible by an IP Address on port 80. Some functionality requires TMS to be reachable by hostname so TMS should also be accessible by a fully qualified hostname as well.
- **Mail Server Access** -TMS requires access to a SMTP (Mail) server to be able to send emails out to users. TMS does not require its own SMTP server and can be configured to use your company's existing mail servers. TMS supports SMTP Auth login for authentication if required. If you are unsure which server to point TMS to, please contact your IT Administrator.
- **Network Access to Managed Devices** – TMS needs specific protocols and access to manage devices. Any network Firewalls or NAT routers must allow traffic to flow to and from TMS. The specific protocols and directions in use will vary based on devices being managed. Please see the TMS Product Support document (available on the TMS installation media) for specific on Firewall requirements for each type of supported device.

Note: Many Anti-Virus programs block applications from sending mail directly using the SMTP Port (TCP Port 25). Please verify your Anti-Virus program configuration and verify it will allow programs to send mail using the SMTP Port (TCP Port 25).

First time setup and configuration of the TANDBERG 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 shall be installed near to the equipment and shall be easily accessible.
- Never install cables without first switching the power OFF.

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 TANDBERG Management Server Appliance is delivered in a special shipping box, which should contain the following components:

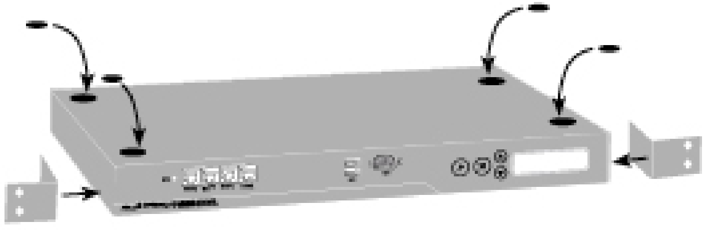
- User Manual and other documentation on CD-ROM
- Rack-ears, screws and screwdriver.
- Cables:
  - Power cable
  - Ethernet cable
- TANDBERG Management Server

Installation site preparations

- Make sure that the TANDBERG 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 Management Server's rear panel and 10cm (4 inches) in front of the front panel.
- The room in which you install the TANDBERG Management Server Appliance should have an ambient temperature between 0°C and 35°C (32°F and 95°F) and between 10% and 90% non-condensing relative humidity.
- Do not place heavy objects directly on top of the TANDBERG Management Server Appliance.
- Do not place hot objects directly on top, or directly beneath the TANDBERG Management Server Appliance.
- Use a grounded AC power outlet for the TANDBERG Management Server Appliance.

Rack Mounting (optional)

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



Before starting the rack mounting please make sure the TANDBERG Management Server Appliance is placed securely on a hard flat surface.

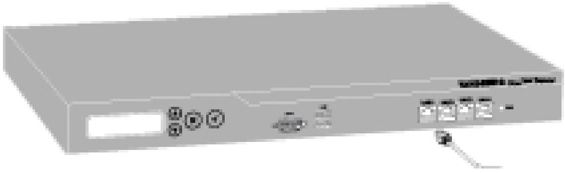
Disconnect the AC power cable.

1. Make sure that the mounting space is prepared according to the ‘Installation site preparations’ above.
2. Attach the brackets to the TANDBERG Management Server Appliance on both sides of the unit using the 8 screws provided.
3. Insert the TANDBERG Management Server Appliance into a 19” rack, and secure with screws in the front (four screws).

Connecting cables

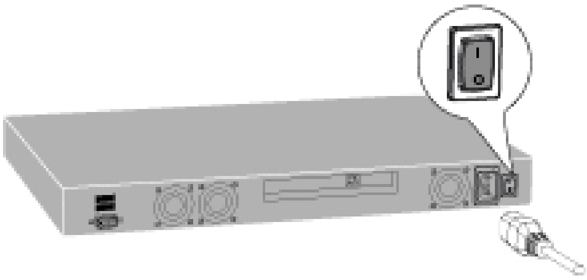
LAN cable

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



Power cable

Connect the system power cable to an electrical distribution socket. Press the power switch button at the back side to ‘1’ to turn on the Management Server. On the front panel of the system the power indicator LED, marked ‘Pwr’, will light up.



NOTE: The Management Server should always be shutdown via the front LCD panel or from the Windows Interface before powering the unit off by unplugging the power cord or power switch.

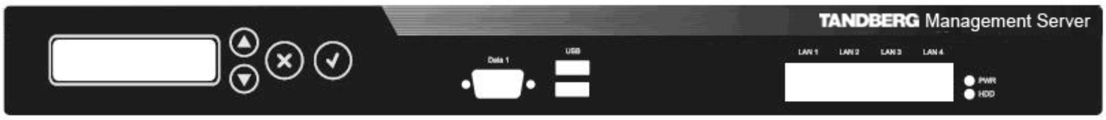
Connecting a Monitor and Keyboard (Optional)

Configuration of the Management Server does not require connecting a keyboard, mouse, or monitor as initial network configuration is done via the LCD Panel. If at a later time direct access to the server is required, you may connect a VGA monitor and USB keyboard and mouse to the server to access the server console.

IP Address Setting Configuration

The TANDBERG Management Server Appliance requires the IP Address Settings to be configured before it can be used. IP Address Configuration can be made using the LCD Panel.

Front view of the TANDBERG Management Server Appliance with 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 the edit mode and confirm selection or entry.
✕	**Return**	Used to return to the previous menu screen or exit the edit mode without saving the latest entry.

Configuring the Server's IP Address:

The LCD panel allows configuration of the server's network address.

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

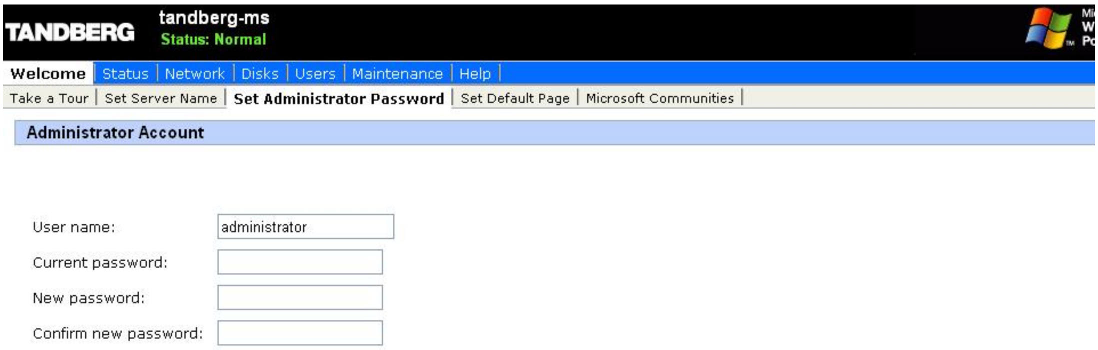
Server OS Configuration

After the server has been configured with a network address, it can be managed over the network connection. To complete the physical installation of the server several basic Server OS settings should be configured.

The server can be configured via the Web User Interface for Microsoft Server. The following steps should be completed from another computer on the network that has the Internet Explorer web browser (ActiveX required) and network access to the Management Server.

1. Start a web browser and enter the address **https://<ManagementServerIPAddress>:8098** where <ManagementServerIPAddress> is the IP address of the Management Server.

2. If you see a security warning stating 'There is a problem with this website's security certificate' – this is normal as your browser does not trust the default server certificate installed. Click the 'Continue to this website' link to acknowledge the warning and continue.
3. When prompted for login, enter the username **Administrator** and password **TANDBERG**.
4. Change the default administrator password. Click the Set Administrator Password menu item under the Welcome tab.


TANDBERG
tandberg-ms
Status: Normal
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:

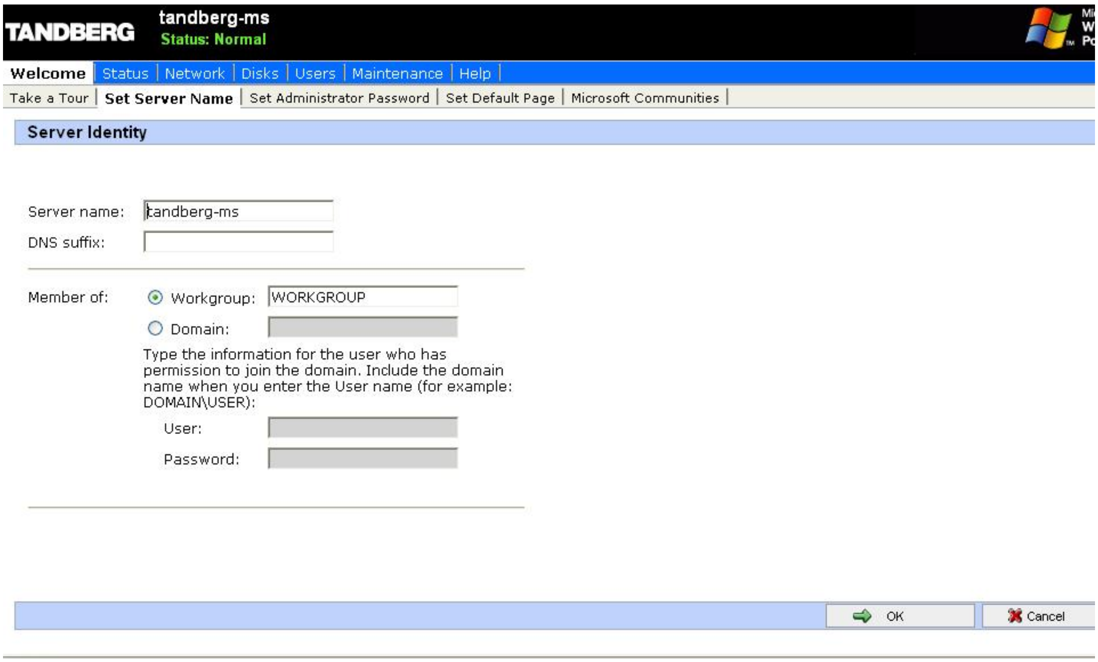
Configure the Administrator Password

The factory default password for the administrator account is **TANDBERG**. This account has full access to the Windows Server OS of the server and therefore it should be assigned a strong, secure password.

WARNING – Do not lose your administrator password! TANDBERG **cannot** recover lost passwords. A server that cannot be logged into as an administrator must be returned to factory for repair and all customer data will be lost.

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

5. Set the Server Time and Time Zone. Select **Maintenance** from the tab menu and click **Date/Time**. On the following page, update the Time, Date, and Time Zone settings and click the **OK** button to save the changes.
6. Configure the server's name and Domain membership. To set the server name and add it to a domain, select the **Set Server Name** menu item under the **Welcome** tab.


TANDBERG
tandberg-ms
Status: Normal
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:

Web Administrator Interface – Set Server Name

The server's default name is tandberg-ms and can be renamed to your preference. Joining the server to an Active Directory domain will simplify user administration by allowing all users of the Active Directory to use their existing Windows Credentials to access TMS. Joining the machine to a domain requires supplying 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 TMS operation.

Make the desired changes and click **OK** to save them. It will be necessary to restart the server to complete any changes to the computer name or domain membership.

7. Finally the server should be checked that it has the latest TANDBERG Server Appliance Security Updates installed. From the factory, the Automatic Updates functionality of Microsoft Windows is turned off. This is by design to avoid any untested changes to the underlying Operating System. To keep the Operating System current and secure, TANDBERG provides regular security updates as self-contained installers for the Management Server. These updates are distributed as 'TANDBERG Server Appliance Security Updates' and are made available to customers via the TANDBERG website at

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

   Download the readme from the above website and verify your Server has the latest Security Updates installed.. Specific installation instructions for the updates are provided with the accompanying ReadMe files.

This covers the essential configuration options that must be done to complete first time setup of the Management Server. For more information regarding the server's setup and ongoing maintenance, please see **Operation, Maintenance, and upgrading the TANDBERG Management Server**.

After completing the first time installation of the Management Server, you continue to **Getting Started with TMS** in this document to continue the initial configuration and setup of the TMS Application.

Operation, Maintenance, and upgrading the TANDBERG Management Server

The TANDBERG Management Server is designed to be a TANDBERG maintained 'black-box' server. Operation of the server is designed to be performed using the LCD Panel or Administrator Web interface, while operation and management of the TMS Application is solely through the TMS interface. Access to the Server OS is available via local console connections or Microsoft Remote Desktop Client but is not required for normal operations.

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

From the factory, the Operating System of the Management Server has been 'locked down' and hardened following the security recommendations of Microsoft for a server of this type. The server does not allow any remote connections except where necessary for TMS communication with users and the devices it manages. The SQL database and other internal components are not accessible remotely. Administrators are discouraged from modifying any settings of the underlying OS.

Basic Server Tasks

Starting and Stopping the TANDBERG Management Server Appliance

The Management Server can be restarted and shutdown via the LCD panel. As with all servers, the Management Server should not be powered off abruptly and restarts/shutdowns should always be performed via the software controls rather than the power switch. Only if the server itself and the LCD panel are unresponsive should the system be power cycled by the power switch. Once a Management Server has been fully shutdown, it is safe to turn off the power switch.

To startup the Management Server

1. The management server requires no administrative input to start up. Simply ensure the power plug is connected, and switch the power switch to 1 (on) to begin the startup. The LCD panel will show the server's current IP address as the startup process nears completion.

To restart from the LCD Panel

1. Press Enter to display the **Main Menu** screen.
2. From the **Main Menu** screen, use the Up or Down arrow to select **Commands**.
3. Press Enter to confirm your selection.
4. From the **Commands** menu, use the Up or Down arrow to select **Restart** and press Enter.
5. You will be asked to confirm this action on the following screen. At the **Restart?** prompt, use the Up or Down arrow to select **Yes** and press Enter to confirm

To shutdown from the LCD Panel

1. Press Enter to display the **Main Menu** screen.
2. From the **Main Menu** screen, use the Up or Down arrow to select **Commands**.
3. Press Enter to confirm your selection.
4. From the **Commands** menu, use the Up or Down arrow to select **Shutdown** and press Enter.
5. You will be asked to confirm this action on the following screen. At the **Shutdown?** prompt, use the Up or Down arrow to select **Yes** and press Enter to confirm

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 from Remote Desktop or using the Web Administrator Interface. To restart/shutdown from the Web Administrator Interface

1. Start a web browser and enter the address **https://<ManagementServerIPAddress>:8098** where <ManagementServerIPAddress> is the IP address of the Management Server.

2. If you see a security warning stating 'There is a problem with this website's security certificate' – this is normal as your browser does not trust the default server certificate installed. Click the 'Continue to this website' link to acknowledge the warning and continue.
3. When prompted for login, enter the username the administrator username and password.
4. Select the Maintenance Tab. Click Shutdown, and on the following page you can chose to shutdown or restart the server.

Performing Database Backups

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. Administrators should follow best practices and take regular backups of their TMS database to ensure they can recover and restore their system in case of a system failure or part of a larger disaster recovery plan.

From the factory, remote SQL access to the Management Server is disabled. Backups can be performed on the server itself via local console or Remote Desktop. Additional help on performing SQL backups is available in the *TMS Database Knowledge Base Tips* document available on the TMS installation media. Backups should be stored offline from the Management Server for maximum protection.

If an administrator wishes to 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's Database Connection properties using the TMSTools application installed in the TANDBERG Program Group on the Management Server.

Operating System Updates

From the factory, the Automatic Updates functionality of Microsoft Windows is turned off. This is by design to avoid any untested changes to the underlying Operating System. To keep the Operating System current and secure, TANDBERG provides regular security updates as self-contained installers for the Management Server. These updates are distributed as 'TANDBERG Server Appliance Security Updates' and are made available to customers via the TANDBERG website at

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

TANDBERG strives to make the security updates that apply to the Management Server available in a timely fashion as Microsoft releases its own monthly security updates.

Register your product at http://www.tandberg.com/support/registration.jsp and you can choose to be automatically notified via email when TMS and TSA Security Updates are made available.

IT IS IMPORTANT THAT YOU DOWNLOAD AND INSTALL ALL SECURITY UPDATES FROM THE TANDBERG FTP SITE BEFORE USING THIS PRODUCT. YOU SHOULD ALSO CHECK THIS SITE REGULARLY TO SEE IF NEW SECURITY UPDATES ARE AVAILABLE. NORMALLY, UPDATES ARE AVAILABLE ON A MONTHLY BASIS OR AS REQUIRED.

TMS Software Installation/Upgrades on the TANDBERG Management Server

The TANDBERG Management Server is upgraded using the same TMS Application software used in software-only installations of TMS. The TMS installer automatically detects if the software is being run on a TANDBERG Management Server and acts accordingly.

The installation or upgrade of TMS software on a TANDBERG Management Appliance is performed using the same steps as a software-only installation, so separate instructions for the Appliance are not required.

To perform a TMS upgrade:

1. Using the Microsoft Remote Desktop Client, connect to the Management Server's IP or hostname.
2. Login using the local administrator username and password

3. The TMS software installer should be copied to the Management Server directly. Using a file share, web download, or the drive mapping feature of Remote Desktop Client, copy the TMS setup file to the server.
4. You may follow the standard TMS Installation and Upgrade Instructions from this point. You should choose the ‘complete’ installation type when given the choice of installation types. Please see **Installation or Upgrade of TMS Software Suite** section of this document for complete instructions for completing the TMS installation.

Note, Tthe SQL Server SA Login information is needed during the upgrade. The factory default for the SQL Login is username: **sa** password: **TANDBERG**

Note: The security policy of the Management Server is updated and maintained by the TMS Installer. If an administrator makes changes to negate any of the security lockdown steps implemented on the Management Server, the security policy will be automatically re-applied when the TMS software installer is ran.

Uninstalling TMS

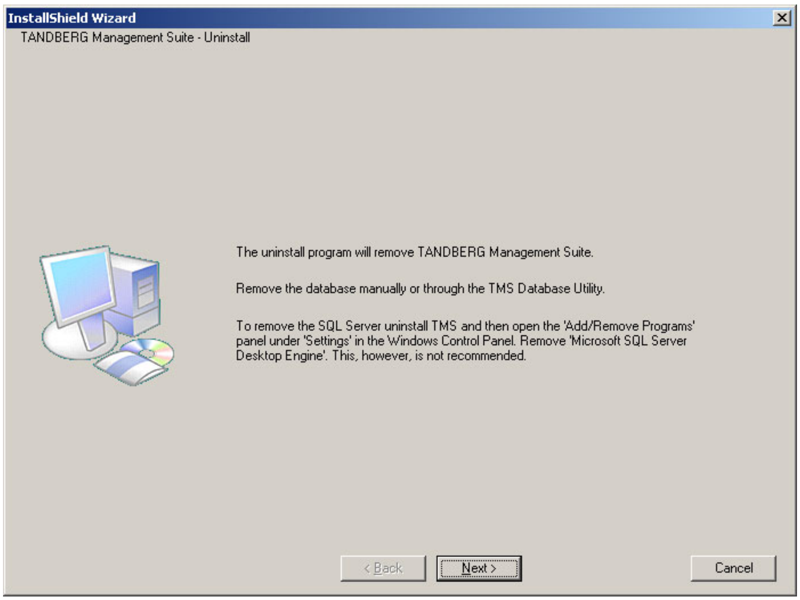
This section will cover the removal of the TMS application. Removing the TMS application is not necessary under normal conditions as the removal of older versions of TMS is handled automatically by the TMS installer software. This information is provided for reference and for advanced troubleshooting.

Uninstalling the TMS Application

Uninstalling TMS will remove the TMS application, website, and services. It will leave any customer data, logs, databases and database servers intact for use in future upgrades. The uninstall wizard will not modify the SQL server in any way. See the next section **Removing all TMS information from a server** if you wish to completely remove all TMS information from the server, including the database servers.

Follow these steps to remove the TMS application:

1. Start the uninstall wizard by selecting ‘Uninstall TMS’ from the TANDBERG Program Group in the Start Menu or by using Add/Remove Programs under the Windows Control Panel.
2. A welcome window will appear that explain that the uninstallation script will remove TMS, but the database and database server must be removed separately. Click **Next** to start the removal process.



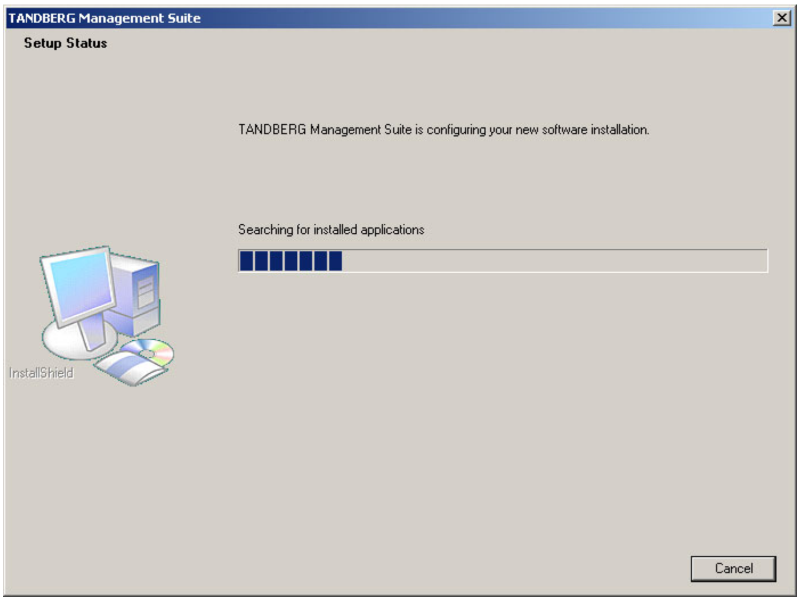
The uninstall program will remove TANDBERG Management Suite.

Remove the database manually or through the TMS Database Utility.

To remove the SQL Server uninstall TMS and then open the 'Add/Remove Programs' panel under 'Settings' in the Windows Control Panel. Remove 'Microsoft SQL Server Desktop Engine'. This, however, is not recommended.

Welcome Screen

3. The wizard will remove the TMS services, website, and application data.



TANDBERG Management Suite

Setup Status

TANDBERG Management Suite is configuring your new software installation.

Searching for installed applications

Removal Process Indicator

4. When completed, you will be prompted to restart your computer. Chose to restart now, or later and click **Finish.**
5. Removal of the TMS application is now complete.

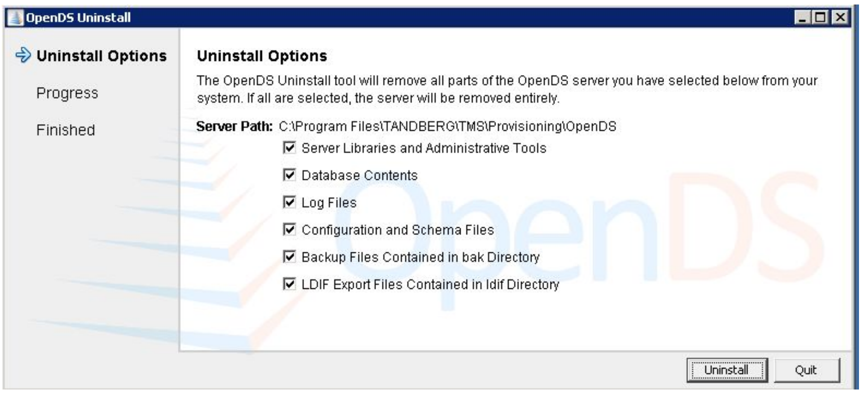
Removing all TMS information from a server

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

NOTE: These steps assume that the SQL server was installed by TMS and is not being used by any other applications and is safe to remove. Do not remove the SQL server or its program folder if the SQL server is used by any other application.

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

1. Complete the TMS uninstall wizard as outlined in the previous section **Uninstalling the TMS Application**
2. Navigate to the Provisioning\OpenDS folder of the TMS installation. Default 'C:\Program Files\TANDBERG\TMS\Provisioning\OpenDS'
3. Double-click 'uninstall.bat'. This will launch the uninstall wizard for the TMS Agent database.
4. Once the wizard starts up, a selection screen will be displayed



Uninstall Options

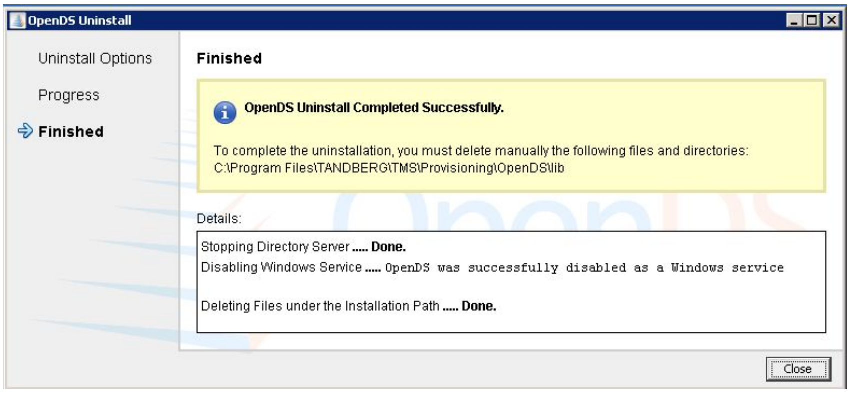
The OpenDS Uninstall tool will remove all parts of the OpenDS server you have selected below from your system. If all are selected, the server will be removed entirely.

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

OpenDS Uninstall Options

5. Ensure all options are checked, and click the **Uninstall** button to start the process. You will receive a warning stating the server is currently running. Click **Yes** to have the wizard stop the service for you.
6. When complete, you will get a confirmation screen showing the database and its files were successfully uninstalled. Click **Close** to complete the wizard.



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:

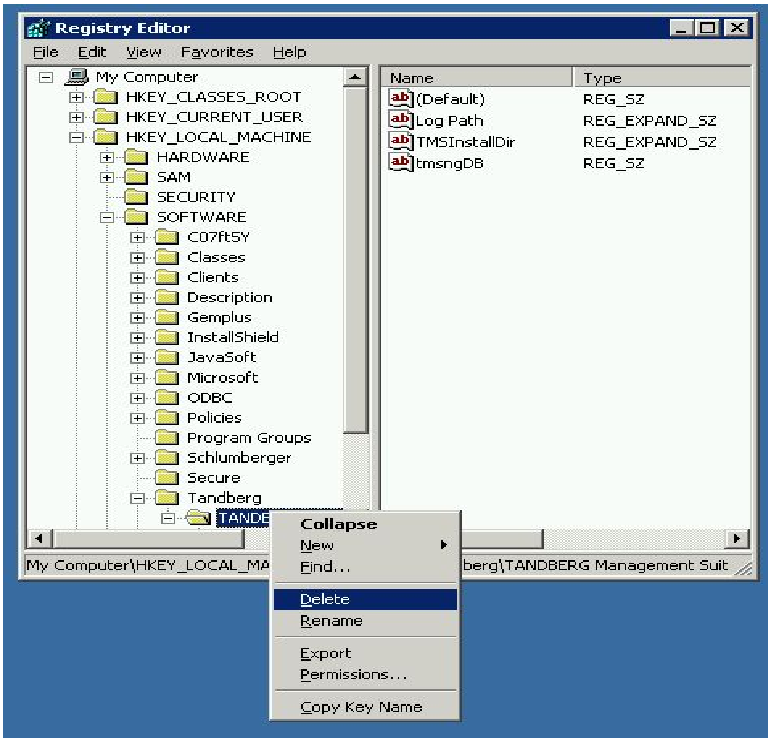
```
Stopping Directory Server ..... Done.
Disabling Windows Service ..... OpenDS was successfully disabled as a Windows service

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

OpenDS Uninstall Successful

7. Delete the program folder used by the TMS installation. The default location is 'C:\Program Files\TANDBERG\TMS'
8. Open the Windows registry editor. From the Start Menu, select 'Run..' and enter 'regedit' and click **OK**.

9. Expand the tree on the left using the plus icons to find the Hive (folder) HKEY_LOCAL_MACHINE\SOFTWARE\Tandberg\TANDBERG Management Suite

10. Right-Click on the TANDBERG Management Suite folder icon, and select **Delete** from the options. You will be prompted if you really want to delete this key, click **Yes**. Close the Registry Editor by clicking the X icon or using the File menu.



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

Deleting the TMS Registry Key

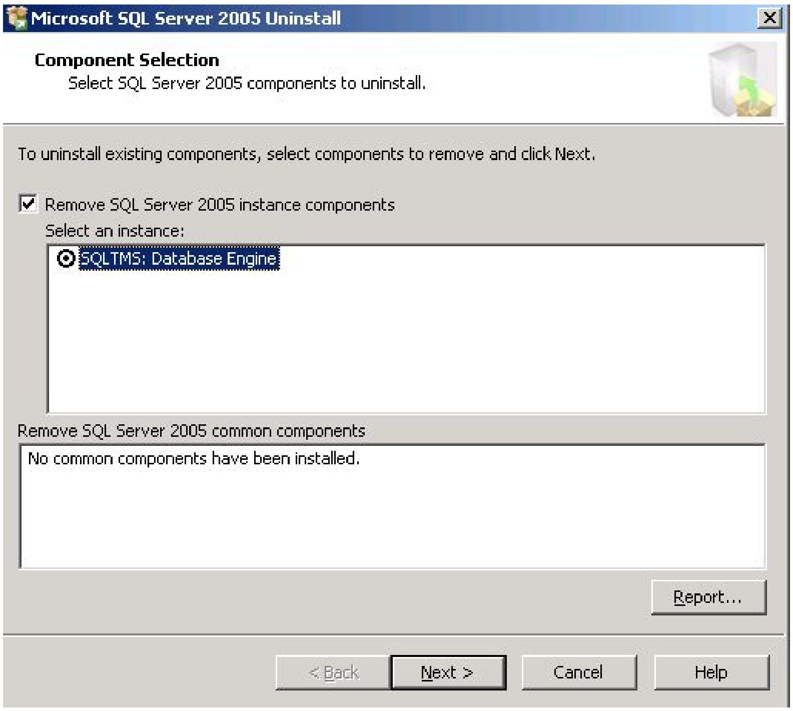
11. If you were using a remote SQL Server, have your SQL Administrator drop the database named 'tmsng'

12. If the TMS installer installed a local copy of SQL Server 2005 Express Edition, complete the following steps to remove it

    i. Open Add/Remove Programs from the Windows Control Panel.

    ii. Find 'Microsoft SQL Server 2005' in the list and click the **Remove** button

    iii. A wizard will open and ask which elements you wish to 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.

SQL Uninstall Wizard

iv. Ensure 'Remove SQL Server 2005 instance components' is checked, and select 'SQLTMS: Database Engine'. Click **Next**

v. You will get a summary page stating that the SQLTMS database engine will be removed. Click **Finish** to start the removal process. The wizard will automatically close when complete.

vi. Delete the program folder used by the SQL installation. The default location is 'C:\Program Files\Microsoft SQL Server'

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

Requirements for Managing Videoconferencing Systems

TANDBERG Management Server supports systems from both TANDBERG and other major videoconferencing vendors. TANDBERG strives to have the best feature parity possible across all supported products. However, due to differences in capabilities and APIs, specific TMS feature and device support is dependent on the individual products and their software versions. Some system types require additional configuration that is unique to that system type.

Due to the immense feature depth of TMS, TANDBERG maintains separate documentation which outlines support for each of TMS's features by product type. The documentation is organized by device categories and product model to make it easy to find your specific system type.

For each model, the following is provided:

- Version compatibility information
- Network requirements between TMS and the system (Firewall Information)
- Device configuration settings that must be enabled to work with TMS
- A table listing each TMS feature and it's support level within TMS

This information is provided in the *TMS Product Support Document* which is available from the TMS installation media and the TANDBERG website. This document is specific to a TMS release, so please be sure to use the revision of the document that applies to your TMS version. This document is updated regularly with new TMS releases or other significant changes.

Getting Started with TMS

The TANDBERG Management Suite (TMS) is a powerful tool for maintaining, operating, and increasing the value of your Conferencing Network. TMS adds intelligence, diagnostics, and functionality well beyond what your individual components offer when operated independently of a management system.

TMS is designed to automate as much of the configuration of the system as possible, and will function for a basic H.323 network 'right out of the box'. However, this baseline configuration is only a starting point, and is not intended to be the final configuration of TMS. An administrator will want to tune TMS's default behaviors to suit their organization's needs, set up permissions for various users, and configure TMS's network model so that all of TMS's call handling functionalities will be available.

This section is intended to help new administrators configure their TMS for first time use and become familiar with some of the tools of TMS. This section is not a reference manual and only covers information needed after first install and some basic understanding of several functions of TMS. It does not cover all features or functions of TMS. For full details on all of TMS's features, please see the *TMS Administrator Guide*.

The section is broken into progressive topics that will walk you through the initial configuration of key elements of TMS will give you a solid foundation to further expand on when time and need arises.

New Installations Verses Upgrades

All new TMS installations should complete the topics of this section before considering their TMS installation 'complete'. For upgrades, these settings will have been completed on a previous installation and are automatically imported into your new TMS installation. However, we recommend upgrade customers also review these topics to ensure their fundamentals are up to date as there may have been new additions to TMS since their original configuration. Please see the TMS Release Notes for a full listing of changes and additions with each TMS release.

Topics

This section is broken into two major categories, configuration and orientation. The topics are progressive - where later steps rely on the previous steps already being completed. A first time administrator should complete all the topics in order. After completing these topics, administrators can move on to further configuring their installation and/or review the *TMS Administrator Guide* for further details.

Configuration Topics

Orientation Topics

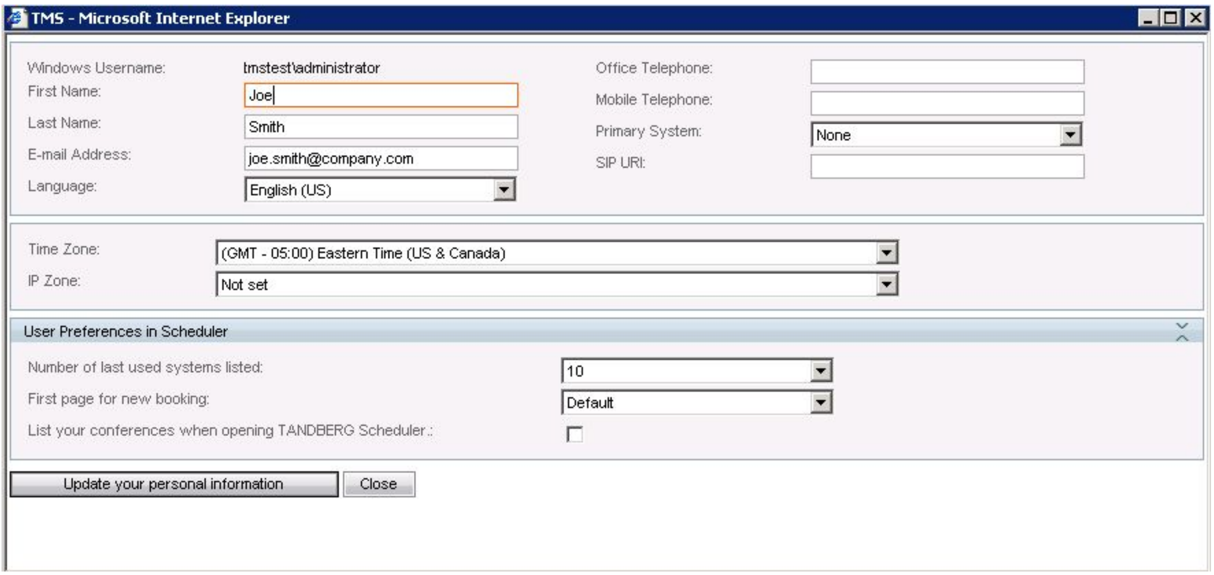
TMS User Concepts

TMS is a web based application, where both users and administrators access the application by simply browsing to the TMS website. But before we discuss how to log into the server, let's first discuss how users are handled in TMS.

To log into the TMS website, 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.

For each user that successfully logs into TMS, TMS creates a user profile for that user based on their Windows username. 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 TMS. While it is possible to create a user profile in TMS manually, this does not create a Windows User account. And vice versa, deleting a user profile in TMS does not alter the user's actual Windows User account, only their TMS profile. A user must always have a valid Windows login to access TMS.

In each user's profile in TMS there are personal information fields such as their Windows username, their first and last name and their email address. These three four fields must be filled in for each user. If not, when the user browses to TMS, a pop-up window will open prompting them to complete their user profile. Each user can chose their own language to use within the TMS Application. The drop-down list includes all the supported languages in TMS. Note: While all languages are supported in the TANDBERG SCHEDULER and notifications, a smaller subset is supported for the main TMS web interface. English, French, Russian, Japanese, Chinese (Simplified) and Korean are the supported languages for the main TMS pages. If another language is selected, that user will see English when browsing pages that do not support their language selection.



TMS - Microsoft Internet Explorer

Windows Username:	tmstest\administrator	Office Telephone:	
First Name:	Joe	Mobile Telephone:	
Last Name:	Smith	Primary System:	None
E-mail Address:	joe.smith@company.com	SIP URI:	
Language:	English (US)		

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.:	□

User Profile Pop-Up Window

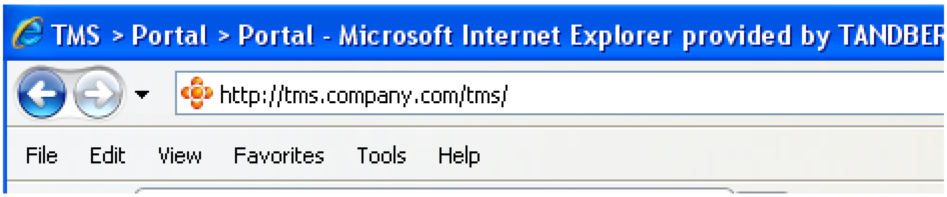
The remaining fields are not mandatory, but are used for other TMS features. Later, if you are using Active Directory, you can configure TMS to populate these fields automatically for new users. It is not necessary to create a user profile for each user manually; the profile will automatically be created the first time the user logs into TMS.

This completes this topic, please continue to the next topic - **Accessing TMS for the first time**

Accessing TMS for the first time

Once TMS is installed, all access to the product is via a web browser. During installation, a TANDBERG Program Group is created in the Start Menu of the server. The 'TANDBERG Management Suite' link in this group provides quick access to the TMS webpage when logged into the server by opening your default browser to http://localhost/tms

TMS is also accessible by simply browsing to the TMS website address. The TMS website is **http://<serveraddress>/tms** where <serveraddress> is the IP Address or hostname of your server.[4]


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

Example: Browsing to the TMS website

If accessing the website from the server console, you will usually automatically authenticate with your currently logged in username and TMS will open. If not, you will be prompted with a username and password dialog box.

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

Domain Users[5]	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 should pop-up after you successfully authenticate. If not, look in your browser for any Pop-Up blocker alerts, and if so, disable pop-up blocking for the TMS website.

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

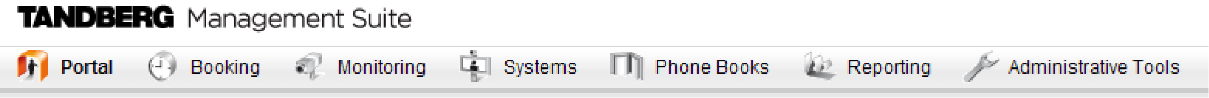
This completes this topic; please continue to the next topic - Moving around TMS and the TMS GUI

[4] Using the server's hostname is recommended as 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.

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

Moving around TMS and the TMS GUI

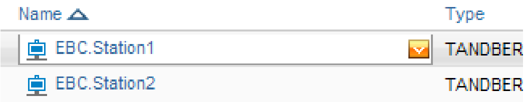
Being the first user to log into TMS, you are automatically an administrator and have full access to TMS. TMS's functionality is grouped by the main categories across the top of the page.

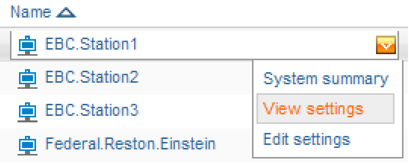


TMS Menu Bar

Navigating around TMS is usually done through these top menu items. Hover your mouse over a menu, and it will expand to show the options under it. Items with triangles next to their name have additional items under that item. Click on an item to jump to that page. The TMS Sitemap under the Portal menu is a single page with links to all the pages in 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. In many places, hovering over an item will display additional tips or information about the item in a tooltip. In other pages, hovering over the item will show the option for a drop down menu. Clicking the orange icon will open a menu to interact with that individual item.



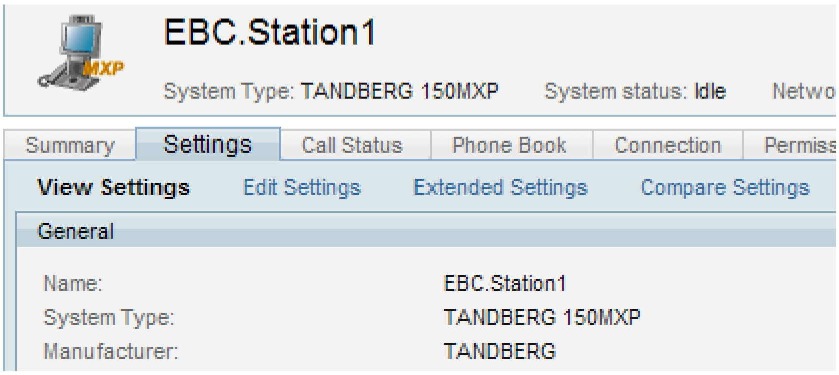


Drop down available **Drop down activated**

The sorting of most lists in TMS can be changed by simply clicking the Title of the column. How a list is currently being sorted can be seen by a small triangle next to one of the column titles. In the images above, the list is being sorted by the Name column in ascending order. Clicking on 'Name' would change the list to descending order. Clicking on 'Type' would change the list to sort by the Type column, etc.

Some lists may have hundreds or even thousands of entries. Rather than show them all in a single list, most lists in TMS are 'paged' where 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 sort through 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 will take to load the web page.

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



System Type: TANDBERG 150MXP
System status: Idle

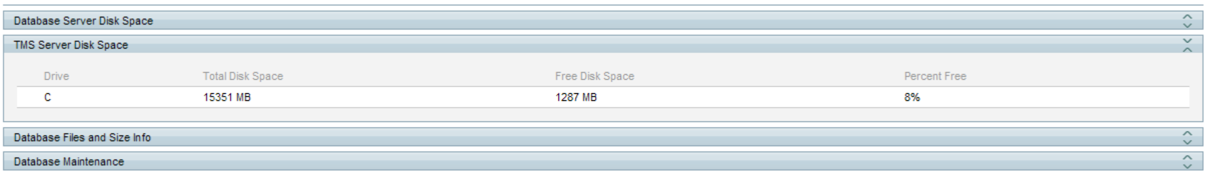
Name: EBC.Station1
System Type: TANDBERG 150MXP
Manufacturer: TANDBERG

Tab Example

In the above image, there are multiple pages available in this view, including Summary, Settings, Call Status, Phone Book, Connection, etc. Setting is the active tab and 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 to show it is the current selection.

Another important concept in the TMS web interface is collapsible panels. A Panel is a surrounded around with a Blue bar at the top. If the bar has arrow icons at the right edge, clicking on the blue bar will cause the panel to either collapse or expand. This allows you to choose which areas of the screen to concentrate on or see more of.



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

Collapsing Panel Example – One panel expanded, with three others collapsed

The last important web elements to highlight are the search and help features. At the top right corner of the TMS web page is a Search box and a question mark. The search box gives a quick way to jump or find an individual system. You can search by name, phone numbers, serial numbers, and more. It's the quickest way to quickly pull up a system for more information. The help icon is available so that when you click on it, a new window will open and automatically take you to the relevant page of the TMS online help system that relates to the page you were on for assistance with using the features on that page.

Now that you are familiar with the way TMS displays information and how to move around, let's setup some basic limits to control who can do what in TMS.

This completes this topic; please continue to the next topic - **Permissions and Groups in TMS**

Permissions and Groups in TMS

TMS gives administrators the ability to control which TMS features users have access to, such as Booking, Device Management, etc. Combined with that, TMS also gives administrators the ability to control which systems users can uses those features with. These feature and system permissions combine for an effective ability per system. 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.

When a user does not have permission to something in TMS, it is normally hidden from their view. So if they have no permission to a system, the system will not even show in their listings. If a user has no Booking permissions, the Booking Menu is not even shown. This allows you to create very simple interfaces for limited role users so they will not be overwhelmed with the full range of features.

TMS controls permissions through the idea of User Groups. Groups are defined in TMS, and users are assigned to groups. What permissions a user has in TMS is based on which groups they are a member and using the permissions each group has. Permissions in TMS are CUMMULATIVE – meaning the effective permission a user has is a sum of all his group permissions.

Groups and permissions are controlled from the User Administration Menu under Administrative Tools in TMS. The permissions each group has is changed by using the **Set Permissions** option when clicking on a Group's name in the Administrative Tools -> User Administration -> Groups page.

TMS starts with several groups created by default, but the most important groups to understand are the **User** Group and **Site Administrator** Group. All users are always a member of the **User** Group, so it is not possible to edit the membership of this group. Any permission given to the **User** group is available to all TMS users. Anyone who is a member of the **Site Administrator** group has full access to all features and systems in TMS. You can edit who is a member of the Site Administrator group, but you cannot edit it's permissions as it always has all permissions. Administrators can and should define more groups to allow greater control of permissions in TMS.

Which groups users are a member of can be set one of three ways:

- The first is by editing the Group itself. The Edit Group Page displays all current members, and by clicking the **Add Members** tab, you can specify which users to add to the group. A user can be a member of multiple groups. A user's groups can also be edited by editing the User under Administrative Tools -> User Administration -> Users
- The second way is by assigning the user to a group automatically when the user's profile is created. TMS does this through 'Default Groups'. Groups set as a 'Default group' will automatically be added to any new user. On first install, the Site Administrator Group is marked as a Default Group. This means any person who logs into TMS, will have a user profile created, and will automatically be added to the Site Administrator group giving them full rights to TMS. This is how you became an administrator automatically when first logging into TMS.
- The last way is through Active Directory Groups. TMS has the option once configured to allow TMS to import existing groups from Active Directory. The Active Directory groups a user belongs to is automatically updated in TMS Groups when the user logs in. This simplifies group administration as it reuses the existing Enterprise Directory and for groups within TMS as well.

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

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

Configure a baseline permissions setup

For initial setup, it is not important to define all your eventual groups, but it is important understand how permission 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 should be done so that new users will not have TMS Administration rights, and you have a default group for new users with a baseline permission set. Administrators can choose if they want their baseline permissions for users to be very strict or generous. The permissions can be changed at any time, but administrators should start planning from the beginning on how access will be controlled in TMS 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 the **New** button to create a new group. Name it appropriately, such as 'All company users' and click **Save**
2. Assign the default permissions you want all TMS users to have in TMS to the new Group. Click on the Group Name in the Edit Group listing, and click **Set Permissions**. Mark the checkbox for each permission you wish group members to have. For a starting point that gives users full access except to TMS configuration, you could check all the boxes except those under Administrative Tools. Use the checkboxes in the blue title bars to mark or clear all checkboxes in that section. Click **Save**
3. Change the Default Groups. Go to Administrative Tools -> User Administration -> Default Groups. Clear all the checkboxes except for the Users Group and your new Group. This means any person who logs into TMS will automatically be added to your new group, and 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 your new group has no permissions marked, and the User Group has all permissions. Clear all the checkboxes for the User Group, and assign the permissions you would like 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 only the users you wish to have Administrator rights are listed. If any other accounts are listed, mark the checkbox of 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 all new users and systems will have the baseline permissions configured on them by default

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

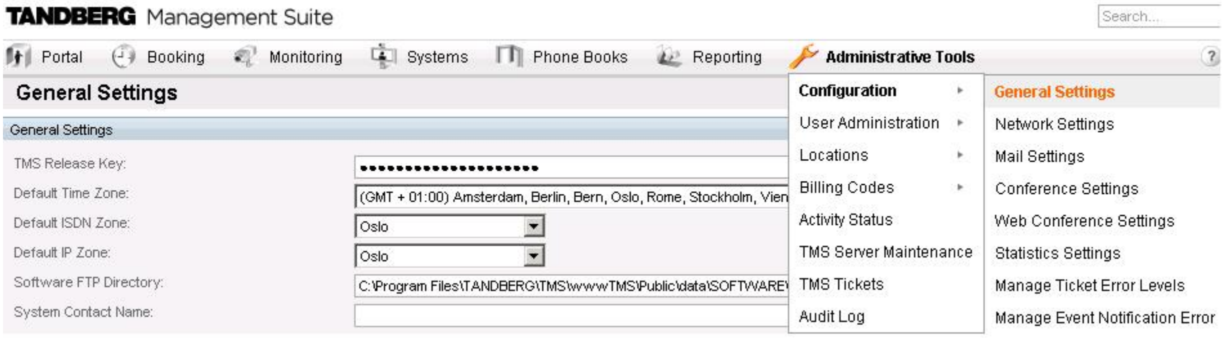
This completes this topic; please continue to the next topic - **Review and Set Important TMS Defaults**

Review and Set Important TMS Defaults

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

This topic will outline the settings you should review and configure at first configuration. For complete details on each setting, please see the online help or the *TMS Administrator Guide*.

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



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:	

Administrative Tools Menu

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

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

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

- **SNMP Community Name** – This is a comma separated list of common SNMP strings TMS will use when discovering and adding systems to TMS. If you use a customized SNMP Community Name on your existing systems, be sure to add it to this list.
- **E-mail Addresses to Receive System…** - You should enter your email address here so TMS can send you notifications about discovering rogue endpoints, system event failures, and other administrative messages. Multiple E-mail addresses can be entered if comma separated.
- **Automatic System Discovery** – By default this is enabled and it automatically adds systems TMS discovers to a folder in System Navigator, and configures their management properties to work with TMS. This makes TMS very simple to setup and get rolling. 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, updating that template is a good place to do it.
- **Active Directory** – These settings allow TMS to leverage Active Directory for its user and group settings. If the TMS server is a member of a domain, it is highly recommended you enable these settings by entering a valid Windows Domain account. The account does not need to be an administrator account, just a normal user account. If **Lookup User Information…** is enabled, when a new user profile is created, TMS will automatically populate

as many of the fields in the user profile as possible from Active Directory. **Allow AD Groups** simplifies TMS Groups by allowing you to use Groups from Active Directory as TMS User Groups which automates which TMS groups a user belongs to. See the *TMS Administrator Guide* for further details on AD Groups. on AD Groups in TMS Groups

- **Scan SNMP Capable Systems to Allow…** - This setting will allow TMS to more quickly detect if a system has gone offline. Enabling this is recommended.
- **SNMP Broadcast/MultiCast Address(es)** – This is the network addresses that were configured in the TMS Installer. TMS will send a SNMP query to these addresses to find new systems. If your network spans multiple networks, add the broadcast address for each, separated by commas to allow TMS to find systems automatically. Do not worry if all networks are not represented here as Systems can also be added manually and through systems contacting TMS.
- **Enforce Management Settings…** - This setting is enabled by default and should remain enabled. This setting is essential to ensure systems are properly configured to point to your TMS server.
- **Advanced Network Settings**

To account for diverse network configurations, TMS supports the notion of two networks that can access TMS. This is used to account for a remote network, such as one outside the organization's firewall or proxy that you may have systems on you wish to manage[6]. These settings are critical because TMS must know its own network addresses to properly configure systems to communicate back to TMS.

The 'local' or LAN network is a network that is normally the same as your organization's internal network. The 'public' network is a second network that can access TMS and is generally used to represent the public internet or a network outside the organization's firewall. Each system added in TMS has a Connectivity parameter that you use to tell TMS which network identity it should use when communicating with the system. The public network addresses are used always used when using the SOHO/Behind Firewall support in TMS.

- **TMS Server IPv4/IPv6 Addresses** – These were configured during installation and should be the IP addresses used to reach your TMS Server
- **TMS Server DNS Address (Local)** – This should be the fully qualified DNS hostname used to access your TMS Server from the internal, or local network of the organization. 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 systems would use to reach TMS.
- **TMS Server DNS Address (Public)** - This should be the fully qualified DNS hostname used to access your TMS server from an outside network if different from the local hostname. This setting must be configured to use features such as SOHO/Behind Firewall support. If the server has no hostname that is usable, enter the IP address the systems would use to reach TMS.
- **Automatic Software Update** – This functionality allows TMS to automatically check over a secure link for new software available for your systems, and notify you of your Service Contract status for your TANDBERG Systems. No personal information is sent during this communication except the system identifying information such as serial numbers and hardware identifiers. If you do not wish to have TMS check for software, you can disable this feature. If your network requires a web proxy to reach the internet, configure the properties for it here.
- **Secure-Only Device Communication** – This is off by default and only should be enabled in specific customer scenarios. Please see the Implementing Secure Management documentation available on the TMS installation media for more information.

[6] 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 should resolve to a IP forwarded to the TMS server's IP address

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

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

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

This completes this topic; please continue to the next topic - **TMS Routing and Zones**

TMS Routing and Zones

To automate conferencing and increase the reliability of conferences, TMS is designed to actively interpret and manipulate dialing information shown to users and systems. This automation relieves the users from trying to understanding calls are possible, if any digits must be added for prefixes or telephone codes, and simply which network protocol to use. All of these decisions are handled automatically by TMS by interpreting the status and configuration of systems it is managing, and an understanding of the network.

TMS's understanding of the network is derived from administratively defined concepts known as Zones. There are IP Zones, and ISDN zones. Zones tell TMS about the network a system is connected to. The administrator defines the zones that represent their network, and systems in TMS are associated to the zone that represents their network. During installation, TMS will have two Zones defined named 'Default' that were created by the installer. These need to be expanded upon to implement a network that goes beyond a single location. Zones are created and managed in TMS under Administrative Tools -> Locations.

ISDN Zones

The job of an ISDN zone is to tell TMS about the ISDN network in a location. A location is simply an area that all has the same ISDN dialing behavior. So a location could represent something as small as a building, or it could be as large as an entire city or state. What is important is that all systems assigned to a zone, share all the same ISDN dialing information. The information that makes up an ISDN Zone is listed below:

- **Country/Region** - Tells TMS which dialing rules to use. Example, do I dial 011 or 00 to dial international calls?
- **Area code** – Used so TMS can make determinations about long distance dialing
- **Line prefixes** – Tells TMS if you must dial any prefix digits before dialing your number – such as dialing 9 to get an outside line from a PBX
- **Digits to dial for internal calls** – Tells TMS how many digits to dial when making calls between systems set to the same ISDN zone. Example, if 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 TMS with regards to local and long distance calling

How many ISDN Zones you will need to represent your network depends on how many different ISDN dialing behaviors you have. To determine if multiple systems can share the same ISDN Zone, simply compare if the above properties are identical between the two systems. If so, they can share the same ISDN Zone.

All ISDN numbers in TMS are stored as 'fully qualified numbers'. Meaning, the number is entered and shown as the full number including its country code information. Example: A US Phone number would be shown as +1 703 7094281. A Norwegian phone number would be: +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 TMS (with ISDN Zones) knows how to manipulate the number so a particular system 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 out of IP network through things like Gateways and URI dialing.

IP Zones are purely logical entities and do not necessarily map to any physical boundary. TMS uses IP Zones to influence its routing decisions as 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 like selecting a MCU – a local MCU may be preferred over a distant MCU. 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 using ISDN when making certain connections, that is also controllable through IP Zones.

For most organizations, the role of IP Zones is to simply provide gateway information for the IP network. The number of IP Zones needed is based on how many different 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 to have phonebooks and scheduling function properly so an understanding of Zones and basic configuration should be tackled as part of the initial configuration of TMS.

Adding Zones for initial configuration

To start a simple network plan, proceed as follows.

1. For each system you will manage that has ISDN directly connected to it (include MCUs, Gateways and endpoints), create one ISDN Zone.

   Before creating a new Zone, consider if an existing zone has the same values. For instance, if you have a MCU, Gateway, and endpoint all in the same building that all use the same ISDN dialing behaviors, they can all use the same ISDN Zone.

   You do not need to create all ISDN Zones now, but you should create ones for the initial systems you plan on working with. Normally adding more ISDN Zones is done before or after adding a new system to TMS, Create ISDN Zones by going to Administrative Tools -> Locations -> ISDN Zones and clicking **New**. Fill in all applicable fields and click **Save**.

2. For each IP Gateway you have (gateways that act as a pooled service can be considered a single gateway), create one IP Zone.

   Under Administrative Tools -> Locations -> IP Zones, click **New** and fill out all the gateway information that applies, including prefixes and DID numbers. Select the ISDN Zone that applies to the Gateway this zone contains.

   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. Click **Save**

3. If you have no Gateways, you still must have at least one IP Zone. A zone named ‘Default’ was created during the installation of TMS and can be used as your sole IP Zone.

4. Once all zones have been created, set which Zones you wish to use for your default for newly added systems. This default is used when systems are added to TMS by Automatic System Discovery. When adding a system manually, this value can be override. You can also change a system’s zones by editing its settings once added to TMS. Go to Administrative Tools -> Configuration -> General Settings. Set the Default ISDN and IP Zone settings to the zones you wish to use as defaults and click **Save**.

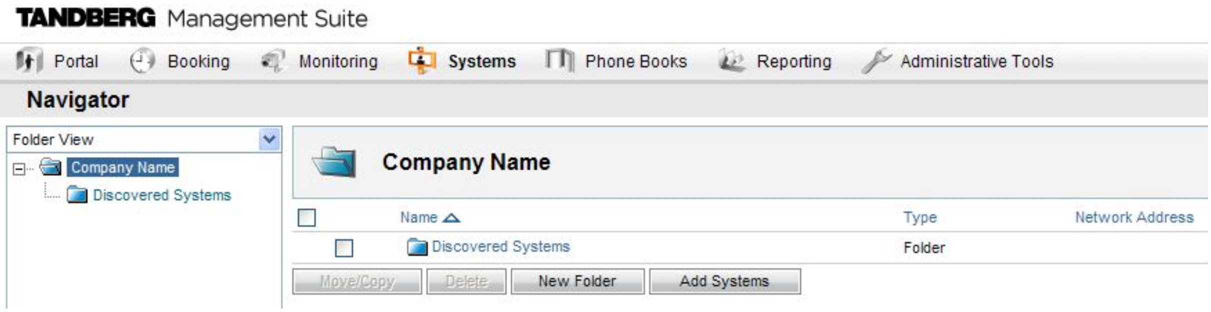
For more assistance with Zones and advanced routing scenarios, please see the *TMS Administrator Guide*.

This completes this topic; please continue to the next topic - **The System Navigator**

The System Navigator

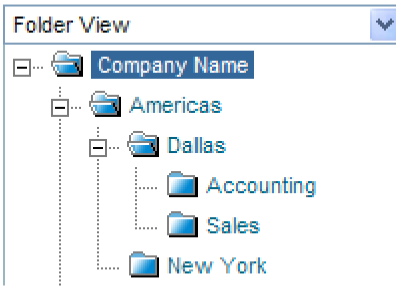
The System Navigator is the 'home' to adding, managing, and organizing systems in TMS. It is found under in the menus as System -> Navigator. The Navigator is essential for all of TMS as it is where systems are organized into a hierarchal structure of folders, similar to your computer's file system. This folder structure, known as the Navigator Tree is used throughout TMS when interacting with systems, including the view of systems users see when Scheduling calls.

Open the System Navigator by going to Systems -> Navigator. In a new installation, there will be two default folders displayed in the list on the left side of the page. A root (top level) folder named Company Name and a child folder named Discovered Systems. The page is organized into two panels, a tree view on the left, and a details panel on the right. Whatever is selected on the left, the details for that item will be shown on the right.



Default System Navigator

Administrators can define any folder structure they like under the root folder. The folders are purely for organizational purposes to make it easier to find systems and to set system permissions. The same folder tree is seen by all users, and is used throughout TMS, so administrators should chose a scheme that is friendly for the users they expect to use TMS. A common model used is one based on geography and organization.



Example Folder Structure

In addition to viewing systems by folder, you can change the tree to display systems by Type, Status, Manufacturer, and other choices. Click on the Drop Down list at the top of the tree to change the view. Adding, moving, or removing systems is only available in the Folder View.

Setup Default Folders

The first step is to rename the default root folder.

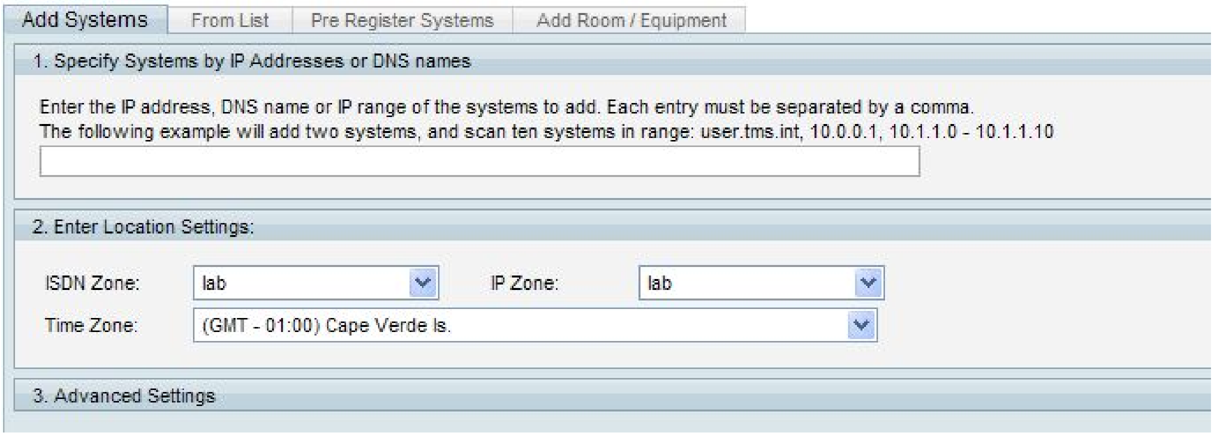
1. Click on the Company Name folder in the tree. The right panel will update to show the contents of that folder. Click the **Edit this Folder** button at the top right side of the screen. Rename the folder with an appropriate Company Name and click **Save**.
2. Next, add any additional folders you wish to add. Folders are not required, but are recommended for organization. You may always add/remove folders at a later time. To add a folder, click on the folder that will be its parent folder in the tree. Then in the right panel click the **Make New Folder** button. Enter a name and description (optional), and click **Save**.
3. Repeat for as many folders as you wish to create.

Adding a System

To manage a system, it must first be added to TMS. As part of your installation, Automatic System Discovery was enabled, and TMS may have already added some systems to the Discovered Systems folder. Click on the Discovered Systems folder, and any systems added will be displayed to the right. We will get back to these systems shortly…

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

1. To add a system manually, navigate to the folder you wish the folder to appear in, and click the **Add Systems** button 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

Add System Page

The Add Systems page is displayed and has several tabs across the top. The first tab allows you to enter a system by entering the system information directly. **From List** displays all the systems that are currently in the TMS database either through discovery or by adding them. **Pre Register Systems** is for adding systems to TMS that may not be online yet. **Add Room/Equipment** is for adding specialized types of systems used in TMS Scheduling. For this example, we will use the manual page to add a system to TMS.

2. Enter the IP Address or Hostname of the system. Select from the drop-downs the Zones you will assign to this system and the Time Zone that the system is located in. Multiple systems can be added at once using a range[7] or comma separated list

   The **Advanced Settings** panel allows you to specify additional details if needed to connect to the system. Clicking on the panel's menu bar will cause it to expand or collapse to see its options. These choices are not needed this example

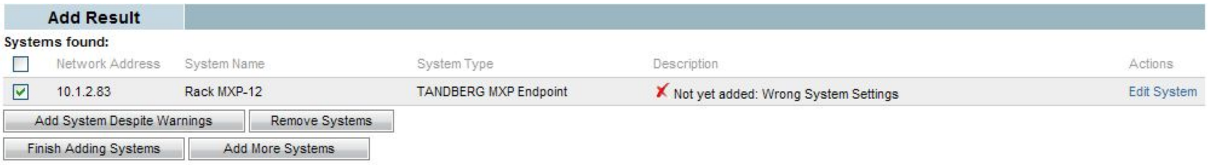
3. Click the **Next** button at the bottom of the page to start adding the system.

   A progress window will be shown as TMS connects to the address and determines the type of system being added, and the system's configuration.

4. If a password is needed to access the endpoint, TMS will prompt you for the system's password. Enter it and click **Next**

   After TMS has successfully contacted and interrogated the system, a Results page is shown with a status for each system it tried to add. As part of the add process, TMS will configure the management settings of the device needed for it to communicate with TMS.

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



Add Result

Systems found:

□	Network Address	System Name	System Type	Description	Actions
☑	10.1.2.83	Rack MXP-12	TANDBERG MXP Endpoint	✗ Not yet added: Wrong System Settings	Edit System

Add System Results Page

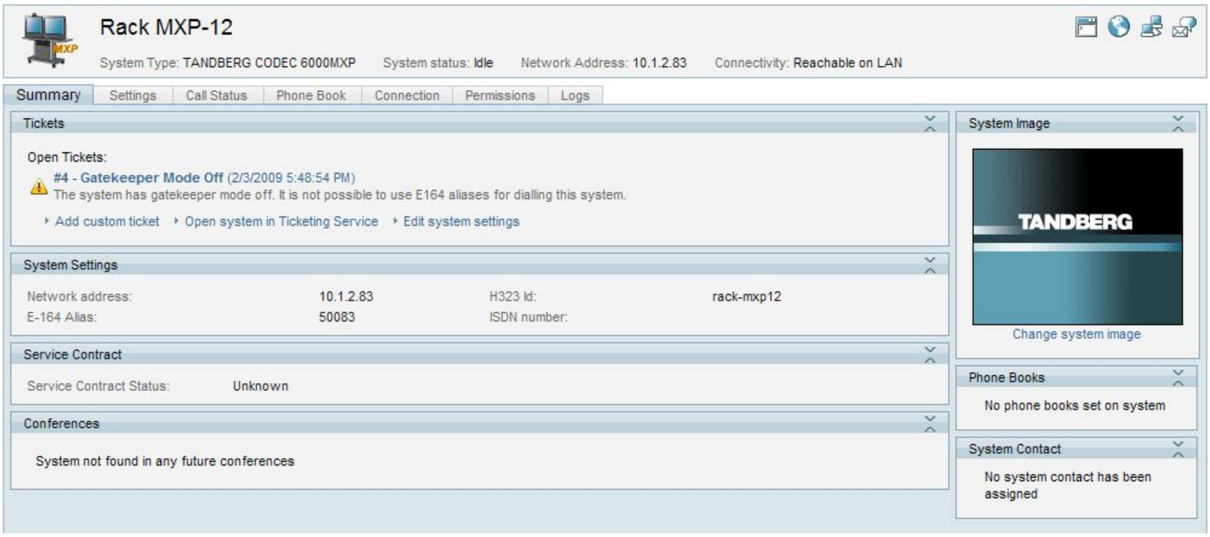
5. If TMS detected problems with a system's configuration, it will display a message in the Description column stating it was not added yet. You can edit the system's settings by clicking on **Edit System**. TMS will display the settings page for the system and a message showing a description of the error. You can chose to edit the settings as necessary and click **Save**. If the problem is resolved, the settings page will close and you will be returned to the Add Results page where the Description has been updated to show the system was successfully added.

   If you do not want to fix the error at this time, or ignore the messages, click **Add System Despite Warnings** on the Settings or Results page will add the system regardless of the existing error condition.

6. Click the **Finish Adding Systems** button to return to the Navigator view. Your new system will now be in the folder's listing.

Viewing and Editing a Managed System

Once added to TMS, a system can be managed from the TMS interface. 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's listing in the right panel. The right panel will update to show the system's 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.

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

Phone Books

No phone books set on system

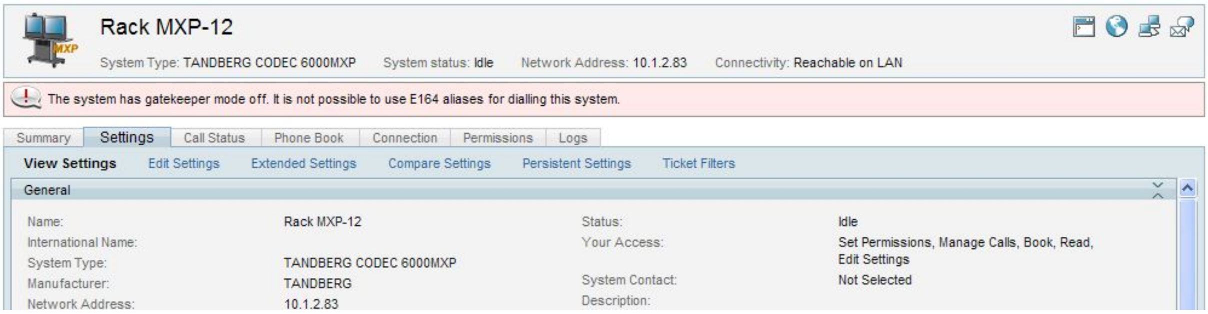
System Contact

No system contact has been assigned

System Summary Page

The default view is the **System Summary** tab. This view gives you an overview of the system and its essential numbers and status. Clicking on the tabs toggles to other views that give more details about the system, such as its settings, active call details, phonebook configuration of the system, connection details for the system and quick access to logs for this system.

Clicking on the **Settings** tab shows a more detailed view of the system's configuration



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.

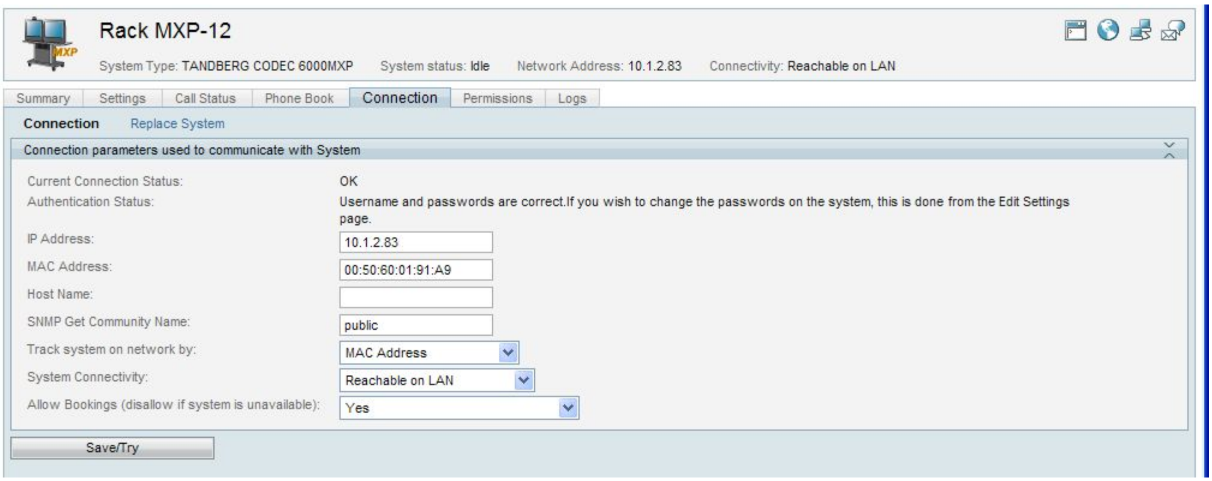
Name:	Rack MXP-12	Status:	Idle
International Name:		Your Access:	Set Permissions, Manage Calls, Book, Read, Edit Settings
System Type:	TANDBERG CODEC 6000MXP		
Manufacturer:	TANDBERG	System Contact:	Not Selected
Network Address:	10.1.2.83	Description:	

View Settings

A **Force Refresh** button at the bottom of the page allows you to force TMS to refresh its view of the system's settings immediately if required.

To edit any of the settings shown here, click **Edit Settings** in the menu bar and you will be able to directly modify the systems settings and the TMS properties for it. It is also possible to restart most systems from this screen by clicking the **Boot** button.

If at any time when using these pages, if TMS is unable to communicate with the system, TMS will display the Connection tab which shows the values TMS uses to communicate 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

Connection Settings Tab

Update any settings as required and click **Save/Try** to have TMS try to reestablish communications with the system.

Update Automatically Discovered Systems

Now that you are familiar with Zones, and working with the System Navigator, you should view the settings of any systems that TMS Automatically Discovered and added to TMS before you completed your initial TMS configuration.

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 necessary.

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

You can also move the systems to a more permanent folder by marking the checkbox next to the system and clicking the **Move/Copy** button when viewing the folder listing.

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

This is only the start of many management possibilities available from the System Navigator, but you are now familiar with how to add systems into TMS and view or change their configuration. Please see the *TMS Administrator Guide* for more thorough explanations of all the management options available in TMS.

This completes this topic; please continue to the next topic - **Configuration Templates**

Configuration Templates

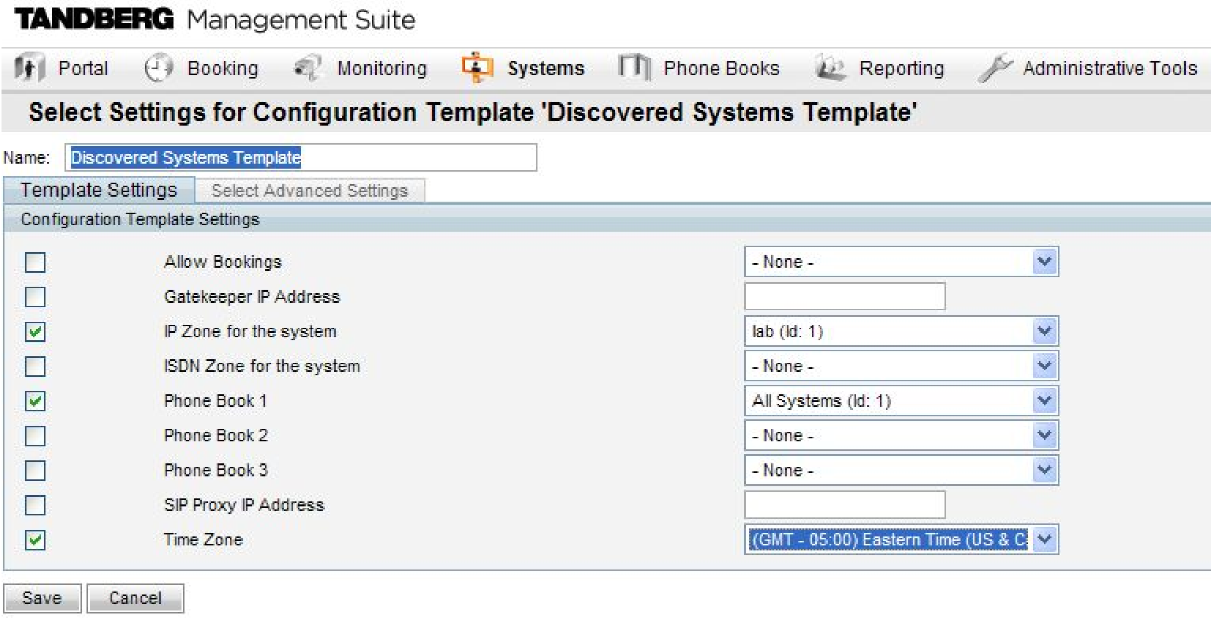
A common administrative need is to apply a common group of settings to one or more systems. This is accomplished in TMS with Configuration Templates. Configuration Templates allow you to define a set of configuration parameters as a set to be applied together to systems. The template can even include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

Administrators can define many different templates, and can apply them to systems manually, automatically when added to 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, TMS created a template for you named ‘Discovered Systems Template’. This template contains a group of settings that are automatically applied to all systems automatically added to TMS by System Discovery. This was done via the **Default Configuration template for Discovered Systems** setting under Administrative Tools -> Configuration -> Network Settings. This topic will review this default as a working example of how to use Configuration Templates.

Editing a Template

1. Open Systems -> Provisioning -> Configuration templates.
2. Click on the template titled ‘Discovered Systems Template’. This will take you to the View Settings page where you can see 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 are of type ‘Other type’ because they are TMS configuration settings, not configuration options from the device’s commands itself.
3. Click on the **Edit** button to see the Edit Settings page.



Select Settings for Configuration Template 'Discovered Systems Template'

Name: Discovered Systems Template

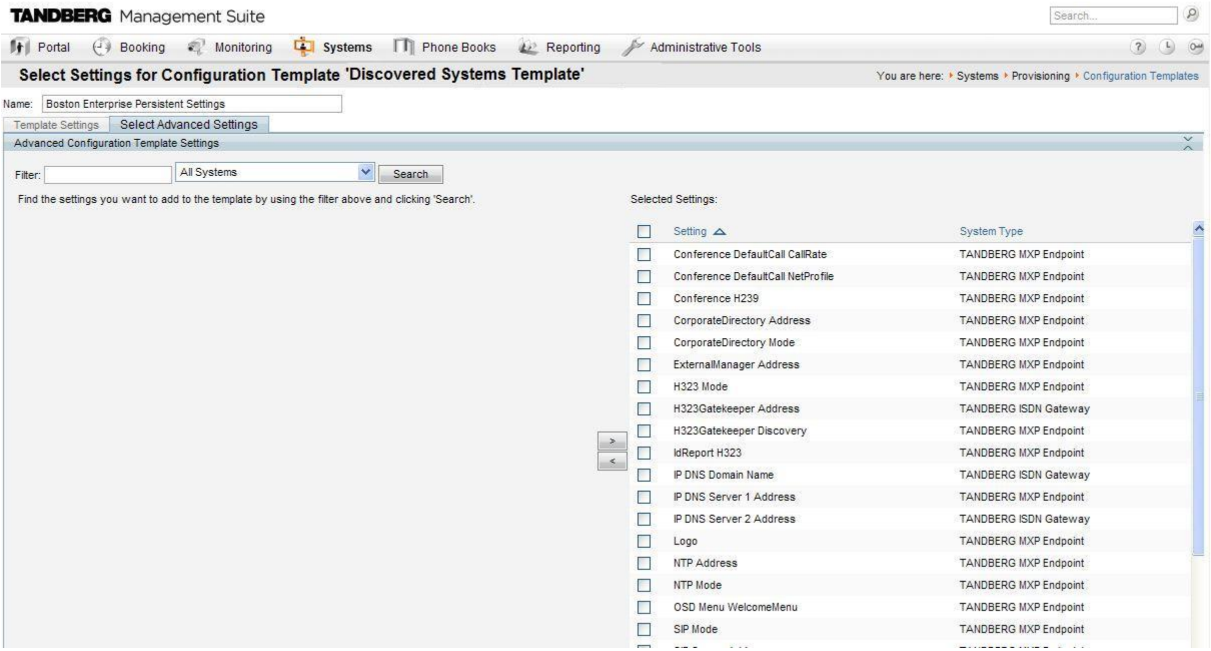
Configuration Template Settings

□	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

Edit Configuration Templates

The first tab shown is the **Template Settings** tab. This tab shows all the settings in the templates and their values. Only settings with a marked checkbox are active in this template. Settings can be enabled or disabled by their checkbox and values updated from the choices on the right.

4. All templates have some common TMS settings added to them to start with, such as Zones and Phone books. To add more settings to the template, click on the **Select Advanced Settings** tab. From this view, you can chose from all the template settings available in TMS and add them to the list to be shown on 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 Search

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

Select Settings for Template

5. The page is split in 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 TMS. The list of available settings is empty when you first enter the tab. Using the Filter box and Type drop-down, you can specify what type of setting you are looking for and hit **Search**.

   Tip: To see a list of all available settings, simply leave the Filter box blank and the drop down set to 'All Systems' and click **Search**

   The list will populate with all the available settings that match the filter criteria.

6. Add or remove settings to the template by marking a setting's checkbox and using the < > buttons to add or remove it from the list on the right.

7. Once the desired changes have been made, click on the **Template Settings** tab to return to the previous view.

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

Creating a New Template

1. To create a new template, click the **New Configuration Template** button at the bottom of the Configuration Templates page at Systems -> Provisioning -> Configuration Templates

2. Enter a name for the template

3. Add/remove settings as described in the previous Edit Templates topic

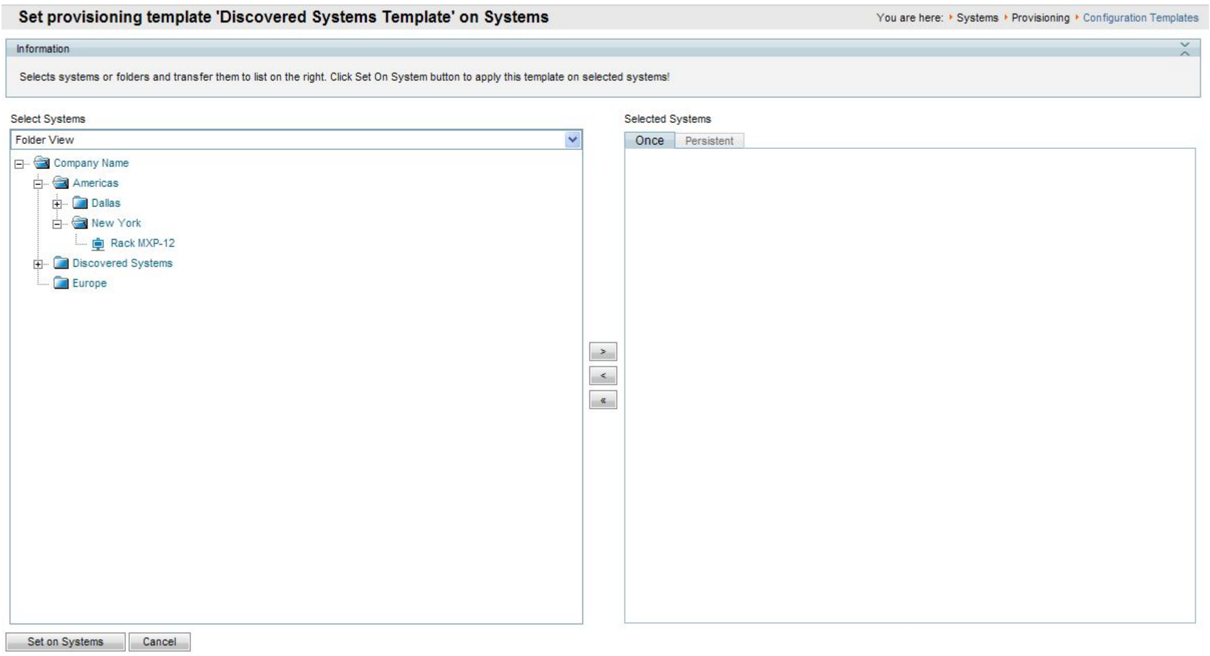
4. Click **Save** to save the template

Applying Templates to Systems

Once created, a Template can be applied to one or many systems at once. 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, do the following

1. Go to the Configuration Templates page at Systems -> Provisioning -> Configuration Templates

2. Hover your mouse over the template name you wish to use, and click the orange arrow to access the drop down menu. Click on **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!

Set on Systems Page

The Set on Systems page displays two lists. The list on the left you will recognize as the tree from the System Navigator. The list on the right has two tabs, Once and Persistent. The Once list will be all the systems that you will apply this template to. See the *TMS Administrator Guide* for more information on Persistent Templates

3. Select a system by clicking on it. Multiple systems can be selected by holding the shift or control keys when clicking on a system. Using the < > buttons to add and remove systems from the Once List.

4. Click **Set on Systems** to start the task. The job of applying the template to systems will take place in the background on the TMS server. You can view status of the job on the Provisioning Activity Status page under Systems -> Provisioning.

This completes this topic; please continue to the next topic - **Phone books**

Phone books

One of the key features of TMS is the ability to offer centralized phone books for managed systems. TMS has the ability to create phone books from a variety of sources including Active Directory, H.350 Servers, Gatekeepers, files, and many more. As part of the initial configuration, you should familiarize yourself with how Phone books are assigned to systems.

In TMS, there are four main concepts to Phone books

- **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 TMS and can be assigned individually to different 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 setup and editable from the local endpoint itself. Server Phone Books are the phone books are created and managed in TMS, not the endpoint or system.
- **External Sources** – These are data sources that can be associated with Phone books to automatically populate the phone book with information from a data source. External Sources can be setup for a multitude of sources including Gatekeepers, Active Directory, H.350 Servers, and other sources. External Sources are created/managed from Phone books -> Manage External Sources
- **Setting on System…** - This is the process that associates a system with a phone book so the system can read and display the phone book's contents. Phone books can be set on any number of systems, and each system can have multiple phone books associated to 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.

As part of the default installation, TMS created a simple phone book that contains all the systems that are managed by TMS and assigned it to all systems TMS automatically discovered. This Phone book is functional example that provides an example of how phone books can be configured and used.

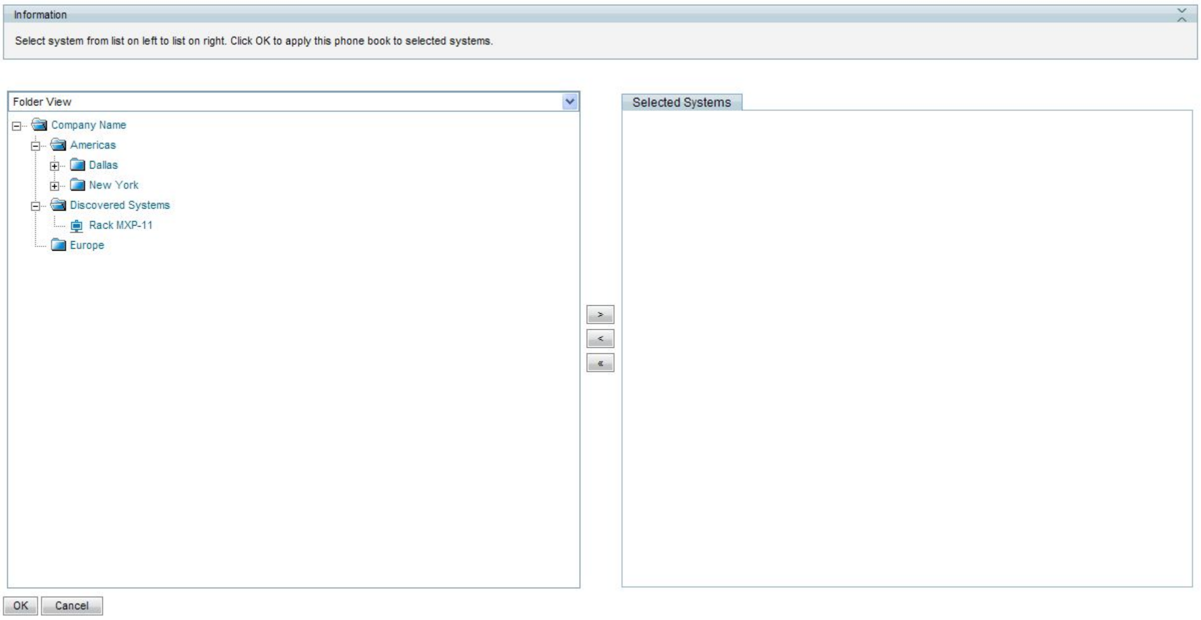
The Default 'All Systems' Phone book

The phone book starts with a list of all the current TMS systems. This list is from an external source that was created during installation.

1. Click on Phonebooks -> Manage External Sources. The source named 'All Systems' is listed with a Type of 'TMS Endpoints'. The type 'TMS Endpoints' will always be up to date with a list of all systems managed by TMS and their contact numbers.
2. Click on **View Entries** to see what data this source currently contains.
3. Open the list of phonebooks by going to Phone Books -> Manage Phone Books.
4. A phone book named 'All Systems' is listed. **Note**: even though this shares the same name as the External Source we just looked at, this is a different object – a phone book.
5. Click on **Connect to External Source**. A list of available External Sources is displayed.
6. There is a marked checkbox next to the 'All Systems source' indicating this phone book will use that external source. The update frequency is set to 5 minutes. So every 5 minutes, this phone book queries the external source to get the latest data from it. Click **Ok** to return to the previous screen.
7. The 'Number of Entries' column shows how many entries are currently in this phone book. Click on **View/Edit** to show the actual contents of the phone book.

   You will see systems listed with a default speed and the IP and/or ISDN numbers of the systems. You can add additional static entries to this phone book if you wish by clicking **New Entries** and entering the information. Click **Save** to save your changes.

8. From the Phone Book listing, click on **Set on Systems** for the All Systems phone book.



Information

Select system from list on left to list on right. Click OK to apply this phone book to selected systems.

Set on Systems Page

9. The Set on Systems page displays two lists. The list on the left you will recognize as the tree from the System Navigator. The list on the right is all the systems that currently have this phonebook set to them.

   You should see that systems that were automatically added into TMS via discovery already have the phone book set to them. This was done via the Discovered Systems Template which was applied when a new system was discovered by TMS.

10. Select a system by clicking on it. Multiple systems can be selected by holding the shift or control keys when clicking on a system. Using the < > buttons in the center you can add or remove systems that will have access to read and display this phonebook.

11. Click **OK** to save your changes and start the task of updating the system's phonebooks.

When you set a phonebook on a system, TMS will automatically configure the phonebook settings on the managed system to work with TMS. The job of applying the changes to systems will take place in the background on the TMS server. You can view status of the job on the Phone books Activity Status page under Phone Books -> Phone Books Activity Status.

This covers the basic example created by the TMS installation. You may create additional Phone Books and External Sources as you desire. Please see the *TMS Administrator Guide* for future details.

This completes this topic; please continue to the next topic - **Scheduled Conferencing**

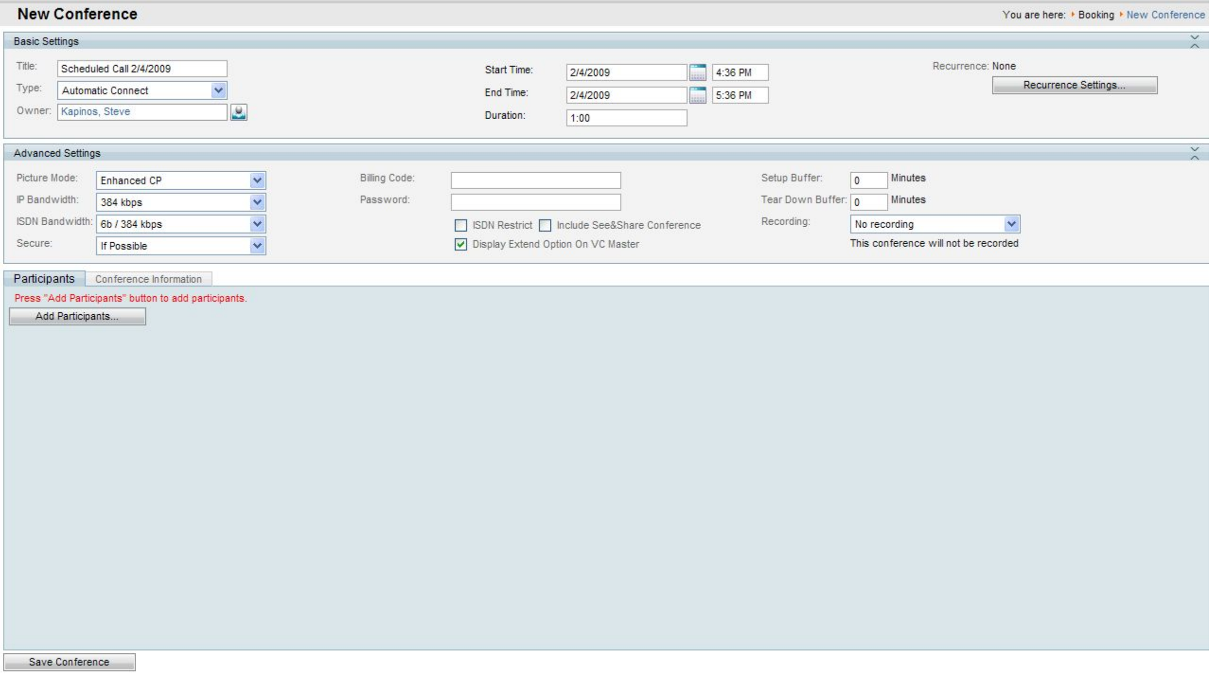
Scheduled Conferencing

With your server's foundation in place, and systems added into TMS, you can now look to add new functionality to your network via automated call launching and control. When scheduling conferences with TMS it is not necessary for the user to worry about network protocols, MCUs, or gateways. TMS handles infrastructure choices and compatibility checking of all these things automatically for the user. For advanced users, TMS allows the scheduler to tune and tweak the conference's selected methods as needed.

TMS offers several interfaces to schedule conferences depending on the need of the user. SCHEDULER is an interface aimed at the mass audience, with administrator defined limits on the settings allowed. Free/Busy Overview is best when you just need to know which systems are available and need a quick meeting. The 'New Conference' page in TMS is the most robust of all the scheduling interfaces and offers all the possible control and settings available in TMS. For this example, we will use the New Conference page in TMS.

Creating your first Scheduled Call

1. Open the New Conference page by going to Booking -> New Conference



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

Press "Add Participants" button to add participants.

New Conference Page

The page is broken into 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 to set additional parameters about the conference such as encryption, recording, or bandwidths. And the bottom section is the most important, where the meeting's participants, and call routing information is presented.

2. Enter a conference Title. This will be seen in all TMS interfaces, and will be seen in the emails sent about the conference

3. Set the conference's start time.

4. Set the duration or end time for the conference.

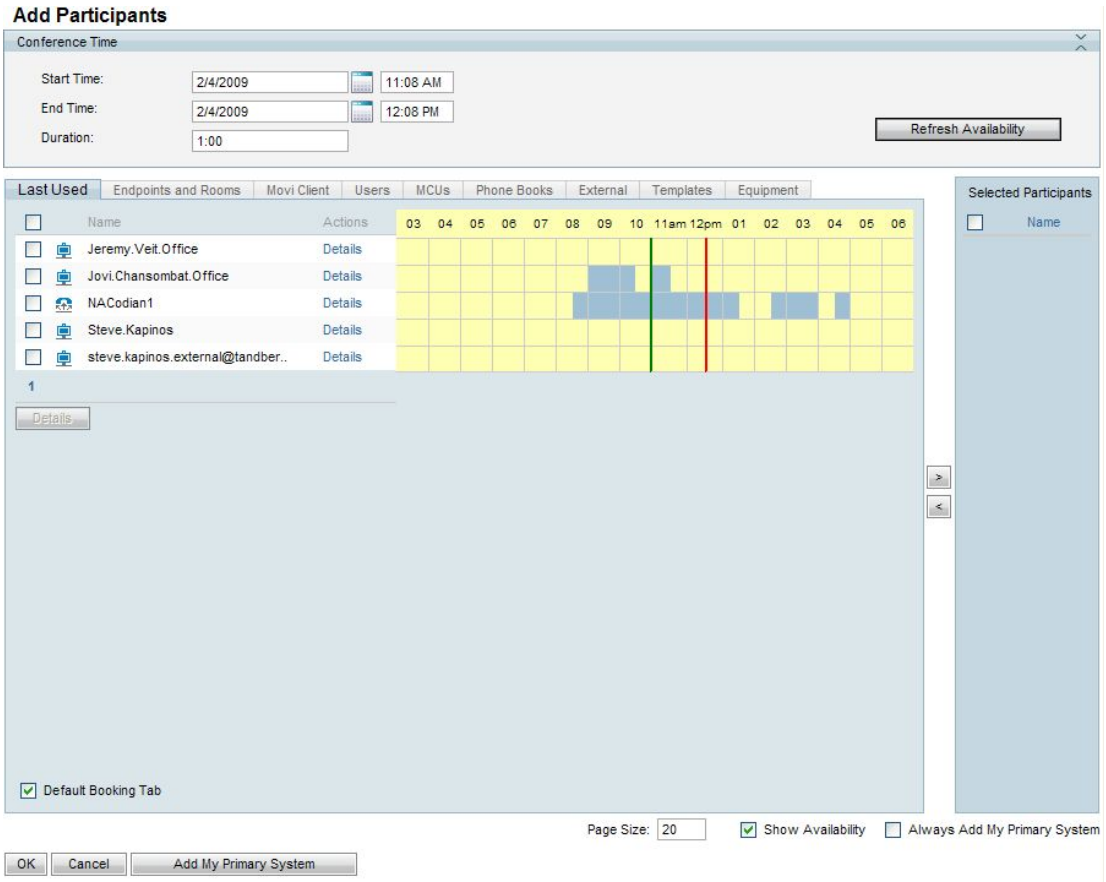
5. The Recurrence Settings button allows you to set a meeting to happen more than once, and create a series of meetings that are tied together. Example: a weekly or daily meeting

   In the Advanced Settings section, you can set configuration options for this one conference. Most settings will take their default values from the Conference Default values you configured under Administrative Tools. We will not cover all the possible options in this example.

- Picture Mode controls the layout the conference will see if you are booking a multiple participant conference. The three choices will map to different layouts depending on the MCU being used. The categories map to these general behaviors: Voice Switched means full screen layouts where one participant is seen at a time; Continuous Presence means multiple participants on screen at a time with equal sized video windows; Enhanced CP means Continuous Presences with unequal sized video windows. This setting can also be changed on the fly while monitoring the conference.
- The bandwidth setting control the speeds at which the calls will be placed, there are separate settings for ISDN and IP speeds.
- Secure controls if encryption will be set on the systems in the conference. If you set it to ‘yes’, TMS will ensure only participants it knows can do encryption will be allowed to be scheduled in the conference.

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

6. The Participant Tab is where you can add participants to the conference. Click the **Add Participant button** and a new window will appear.



Add Participants

Conference Time

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

☑ Default Booking Tab

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

Add Participants Window

The Window Displays lists of available participants and a planner view showing their availability based on existing scheduled and ad-hoc meetings. The colored vertical lines represent your current requested time for the scheduled meeting.

The tabs running across the window show all the available types of participants you can select from. The default view if you’ve used Scheduling before is a ‘Last Used’ tab giving you quick access to the systems you’ve used recently. New users would be interested in ‘Endpoints and Rooms’, MCUs’, ‘External’, and Phone Books. Each lists all the available participants from that category.

When a category is selected by the tabs, the list of available participants will update showing their availability. Hover over any system, or the blocks in the planner view for additional details about the system or scheduled meeting.

7. Add participants to the meeting by marking their checkbox and clicking the > button to add them to the list of selected participants on the rights side of the window. **Note**: It is not required to add any network infrastructure components like MCUs, or Gateways. TMS will handle this for you automatically.

   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, you enter their contact information, and TMS will automatically connect them to the conference at the scheduled time. For dial-in participants, TMS will reserve the capacity needed to host the site in the conference and will provide you with precise dial-in information to forward to the participant.

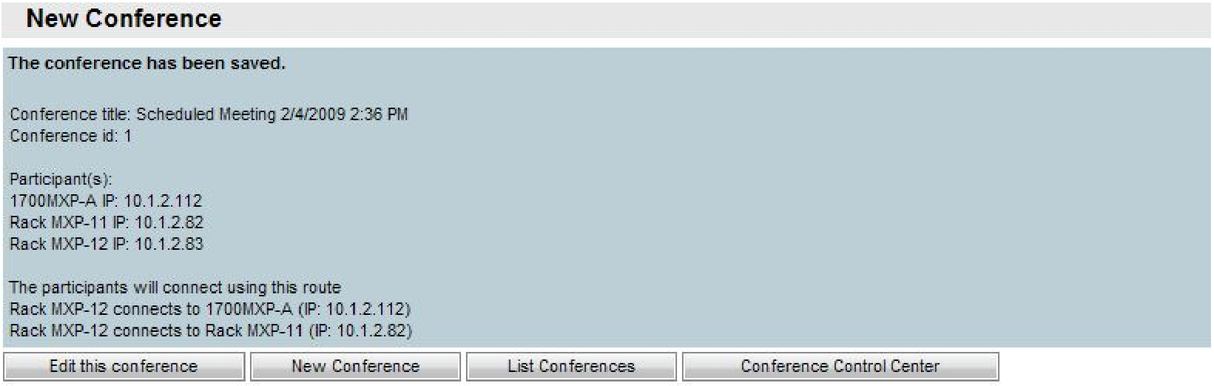
   Once all participants have been added, click **OK**.

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

8. The Video Conference Master drop down controls which system should be considered the meeting organizer. This system will be the one TMS uses to ask if the meeting should be extended when it's about to expire, or to connect the sites if the conference is not scheduled to be an Automatic Connection. Update the Conference Master if necessary. **Note**: TMS will only show participants in this list that are compatible with the onscreen messaging features of TMS.
9. Click **Save Conference** to save the conference. When the conference is saved, TMS will do all 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 as needed.

If 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, TMS will return you to the New Conference page and display a message banner stating why it was not possible to save the meeting. You can edit the conference settings to try to resolve the issue and try saving the conference again.

10. If TMS is able to complete your request, you will be presented with a Confirmation page showing the details of your meeting, including the participant list and listing how each of those participants are scheduled to connect to the conference, including the exact dial string any participants must dial. The Conference ID is a unique identifier for a conference that is valuable for 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)

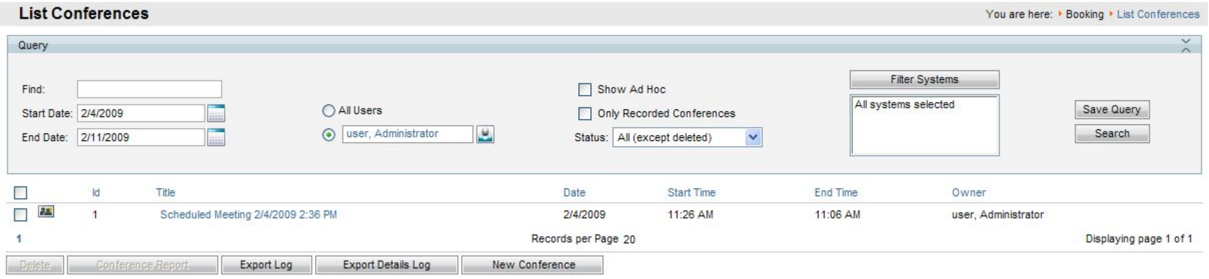
Conference Confirmation Page

You will also get a E-mail 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 to view past or future conferences. From this view, you can see all the settings that were configured for the conference, the route TMS built to connect the call, and a log of events for the conference. If the conference is scheduled for a time in the future, you can also edit the conference to change its settings.

1. Open Booking -> List Conferences



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

List Conferences Page

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**

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

The resulting page will look like the New Conference page, except you cannot make any changes. Click on the tabs in the lower segment of the window to see all the different information saved for this conference, including a log of events, and the Connection Settings tab which will show you how the call was scheduled to connect between the participants.

If the conference is scheduled for the future, you can click the **Edit** button and modify the meeting using the same options that were available to you for creating a new conference. Upon saving the conference, it will replace the previous version and send out new scheduling confirmation E-mails.

This completes this topic; please continue to the next topic - **Monitoring and Managing Ongoing Conferences**

Monitoring and Managing Ongoing Conferences

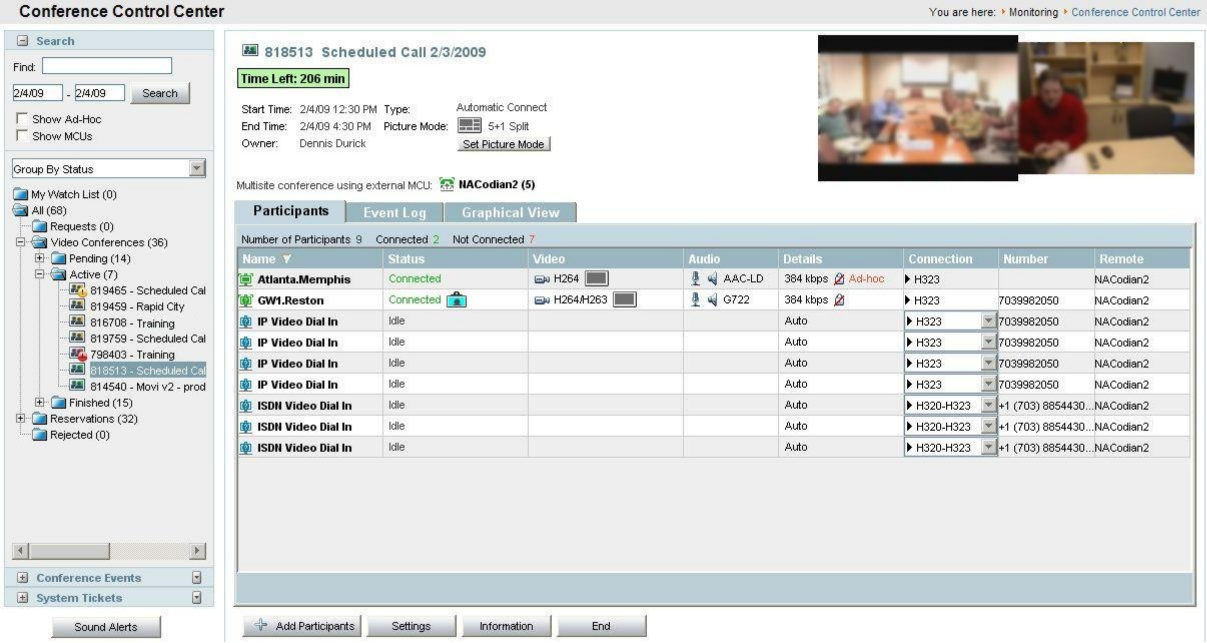
Not only does TMS automate and centralize the process of creating conferences for a diverse conferencing network, it also allows you to monitor and actually control those conferences in real-time.

By monitoring the managed systems on the network, TMS is able to give you graphical displays and controls of both scheduled conferences (Conferences initiated by TMS) and ad-hoc conferences (Conferences initiated by users at their own systems).

The most advanced views and controls for these conferences are available from the Monitoring menu in TMS. This menu has three interactive real-time applications to work with.

Conference Control Center

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



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 Type: Automatic Connect
End Time: 2/4/09 4:30 PM Picture Mode: 5+1 Split
Owner: Dennis Durick

Set Picture Mode

Multisite conference using external MCU: NACodian2 (5)

Participants | Event Log | Graphical View

Number of Participants 9 Connected 2 Not Connected 7

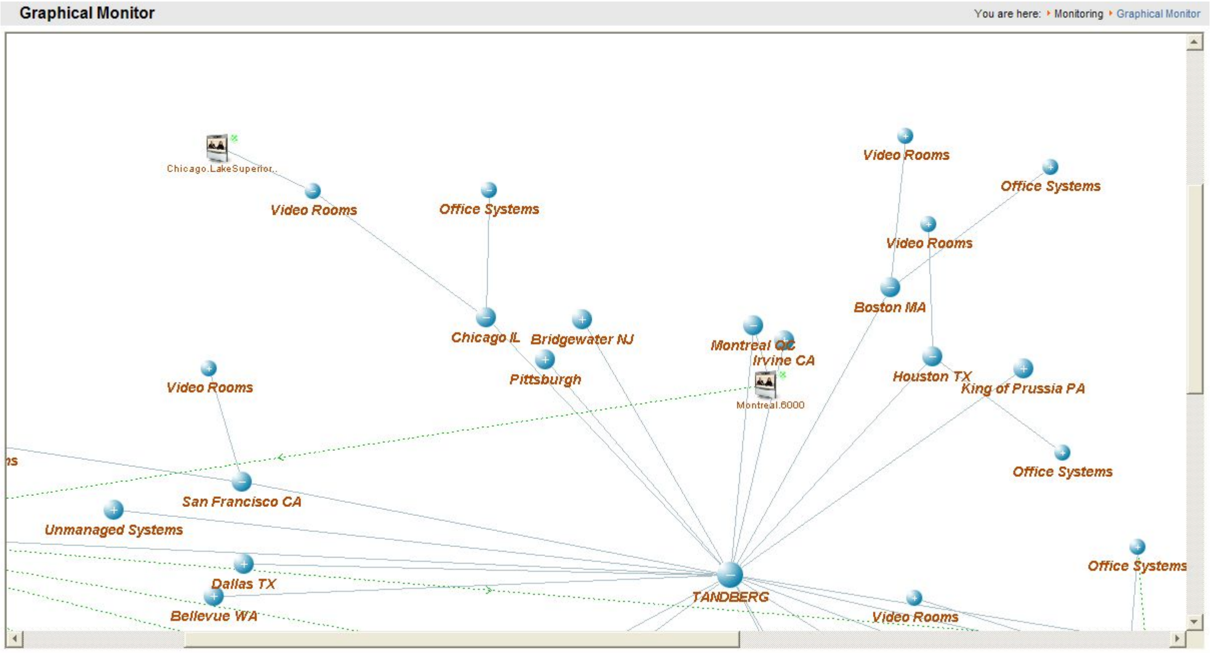
Name	Status	Video	Audio	Details	Connection	Number	Remote
Atlanta.Memphis	Connected	H264	AAC-LD	384 kbps Ad-hoc	H323		NACodian2
GW1.Reston	Connected	H264/H263	G722	384 kbps	H323	7039982050	NACodian2
IP Video Dial In	Idle			Auto	H323	7039982050	NACodian2
IP Video Dial In	Idle			Auto	H323	7039982050	NACodian2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

Add Participants | Settings | Information | End

Conference Control Center

Graphical Monitor

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



Graphical Monitor

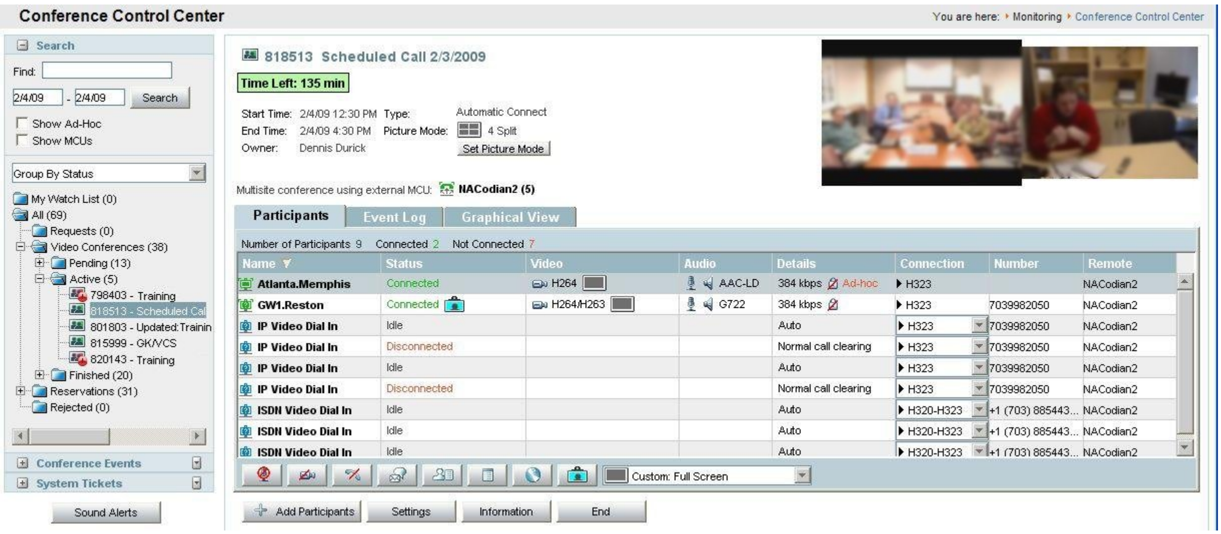
Graphical Map Monitor

The Graphical Map Monitor is a variant of the Graphical Monitor where instead of all systems being shown on one page, each folder has its own page and administrators may overlay graphics behind the icons and images. This is very useful for showing geography or system location information.

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 offers information about upcoming calls, and performs diagnostics on ongoing conferences to alert you via sound and colored icons about the status of your ongoing conferences. These diagnostics allow conference operators to monitor large numbers of conferences across the entire network simultaneously without having to try 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 one will open the conference in the Details panel to the right.



818513 Scheduled Call 2/3/2009

Time Left: 135 min

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

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

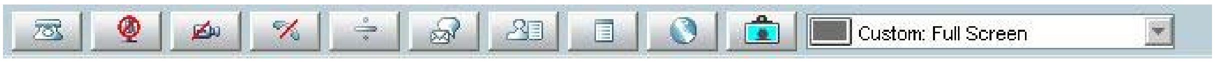
Viewing a Conference

In the Details panel, you have access to view the status of the call, video snapshots from the call, activity logs from the call, and 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 will update automatically as you monitor the conference.

Clicking on site will show icons across the bottom of the list that you can use to interact with the site. You can also right click on the site, and get the same options in a contextual menu. Here you can do things like disconnect, reconnect, mute, get details about the site, or even change the conference layout the participant is seeing.



Participant Controls

The **Event Log** tab will show a history log of the conference, which shows 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, or End the conference.

This completes this topic; please continue to the next topic - **Reporting**

Reporting

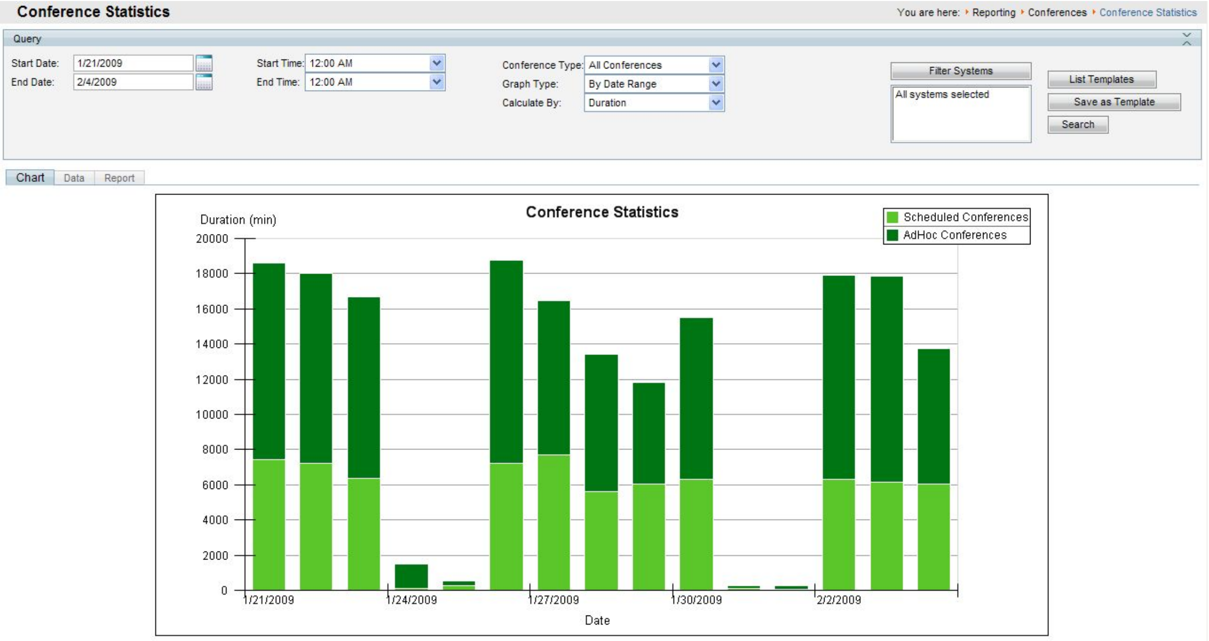
TMS is always collecting data from the systems it manages as well as logging activity that takes place in TMS itself. The Reporting section of TMS gives administrators the ability to visualize and review historical data from their conferencing network.

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 your actual conferencing usage.

Reports in TMS are available under the Reporting menu and are broken into several categories to represent the different reports that are available. TMS offers numerous reports which can displayed which we will not review here, but they all use the same basic interface to interact with the reports which we will cover.

Immediately after install, these reports will not be interesting to look at because there is no history of data to review. The example below will show you an example report to familiarize yourself with the features of the reporting pages. You should look at your Reports after TMS has been installed for a period of time to explore data from your own network.

An Example report from the Conferencing Statistics Report is shown below



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

Example 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 by clicking **Save as Template** to reuse later if you frequently look at the same report.
- **Chart View** – Shows you a graphical representation of the data. The chart type will vary depending on the data being displayed, including line, bar or pie charts.
- **Data view** - Shows you the actual data that makes up the report, such as the call history, event log, or conference history in a table format. This information can be exported to Excel by clicking the **Export to Excel** Button for further analysis.
- **Report View** - Puts the Chart view into a presentation format that can be exported to a PDF file by clicking **Export to PDF**

This completes the Getting Started section of the document. Please see the *TMS Administrator Guide* and Online help for further instructions.

Contact us

If you have any questions, comments or suggestions, please see the Online Support service at www.tandberg.com

It is also possible to send a fax or mail to the attention of:

Product and Sales Support
TANDBERG
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 TANDBERG, Norway. We are committed to maintain a high level of quality in all our documentation. Towards this effort, we welcome you to Contact us with comments and suggestions regarding the content and structure of this document.

Trademarks and Copyright

Contains iType™ from Agfa Monotype Corporation.

AGFA | Monotype

Disclaimer

The information in this document is furnished for informational purposes only, is subject to change without prior notice, and should not be construed as a commitment by TANDBERG. The information in this document is believed to be accurate and reliable; however TANDBERG assumes no responsibility or liability for any errors or inaccuracies that may appear in this document, nor for any infringements of patents or other rights of third parties resulting from its use. No license is granted under any patents or patent rights of TANDBERG.

Environmental Issues

Thank you for buying a product, which contributes to a reduction in pollution, and thereby helps save the environment. Our products reduce the need for travel and transport and thereby reduce pollution. Our products have either none or few consumable parts (chemicals, toner, gas, paper) and low energy consuming products.

Waste handling

There is no need to send any products or material back to TANDBERG as there are no consumables to take care of. Please contact your local dealer for information on local waste handling and recycling of electronic products.

Production of products

Our factories employ the most efficient environmental methods for reducing waste and pollution and ensuring the products are recyclable.

Digital User Manuals

TANDBERG is pleased to announce that it has replaced the printed versions of its User Manuals with a digital CD version. The environmental benefits of this are significant. The CDs are recyclable and the savings on paper are huge. A simple web-based search feature helps users directly access the information they need. If desired, the user manuals on the CD can still be printed locally.

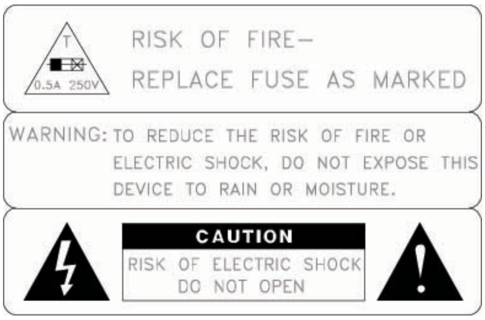
Operator Safety Summary (Appliance)

For your protection, please read these safety instructions completely before operating the equipment and keep this manual for future reference. The information in this summary is intended for operators. Carefully observe all warnings, precautions and instructions both on the apparatus and in the operating instructions.

Equipment Markings

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

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


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 - Most systems should only be used with a cart, stand, tripod, bracket, or table specified by the manufacturer, or sold with the apparatus. When a cart is used, use caution when moving 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

Appendix 1 – Installing TMS on Windows 2008

The TANDBERG Management Suite (TMS) is compatible with 32bit editions of Windows Server 2008. Windows Server 2008 includes Internet Information Services (IIS) version 7 and a new Windows Firewall. These changes introduce some steps that require administrator intervention to successfully install and operate TMS. This document will provide the information necessary to use TMS and Windows Server 2008 successfully.

This section is broken into three topics

- Background Information
- Required Steps to Install TMS on Windows Server 2008
- Restricting IIS 7 Modules to minimal required (Optional)

The first two topics should be read by all Windows Server 2008 administrators and are required to install TMS properly. The third topic is optional and is provided as reference information for administrators that wish to explicitly define and limit which IIS modules are required by TMS.

Background Information

The TANDBERG Management Suite (TMS) is compatible with 32bit editions of Windows Server 2008. Windows Server 2008 includes Internet Information Services (IIS) version 7. IIS7 is a significant advancement for the Windows Server platform in the degree of control it allows an administrator to have over the IIS installation.

Windows Server 2008 introduces two items that must be addressed by an administrator to properly install TMS.

IIS 7 not automatically installed

Due to some of the changes with IIS7, the current TMS installer cannot automate the installation of IIS as it has done for previous IIS versions. This simply means IIS must be installed on the server prior to installing TMS. IIS is a standard component of Windows Server 2008 but is not installed by default.

Default Firewall Rules

Windows Server 2008 includes a new Windows Firewall Program that can control both inbound and outbound ports and is enabled by default. If an Administrator wishes to leave the Windows Firewall enabled, the ports required for TMS must be opened. The full list of ports used by TMS is listed in the steps below and must be enabled in the Windows Firewall.

Required Steps to Install TMS on Windows Server 2008

NOTE: Windows 2008 64bit is not supported at this time.

If you had previous attempted to install TMS on the server, uninstall TMS by choosing the Uninstall TMS option from the TMS Program Group in the Start Menu before proceeding.

1. Open Server Manager from the Start Menu. Start Menu -> Administrative Tools
2. From the Tree list in the left panel, select **Roles**
3. In the center panel, click **Add Roles**
4. A Before You Begin information screen may appear, click **Next**
5. A list of Server Roles will be displayed. Mark the Checkbox for **Web Server (IIS)**

   NOTE: A prompt may appear that several Windows Product Activation Services are required, click **Add Required Features** if prompted to accept those requirements.

6. Click **Next** and an *Introduction to IIS screen* is displayed. Click **Next**

   A list of Role Services will be displayed. By default, Windows will have a minimal list of services enabled. Additional services must be enabled for TMS to operate. Below is a list of the services that are **required** for TMS to operate. Additional Services may be installed at the Administrator's discretion or to support other applications, but will increase the attack surface area of the server. This list only encompasses TMS's needs but should be followed as long as TMS is the only web application on the server.

   NOTE: When selecting some services, you may be prompted that other services are required for this service, Click **Add Required Features** if prompted to accept those requirements.

7. Ensure the checkbox is marked for **each** of the services listed below

   - Common HTTP Services
     - Static Content
     - Default Document
     - HTTP Redirection
   - Application Development
     - ASP.NET
     - .NET Extensibility
     - ASP
     - ISAPI Extensions
     - ISAPI Filters
   - Health and Diagnostics
     - HTTP Logging (recommended)
   - Security
     - Basic Authentication
     - Windows Authentication
     - Digest Authentication
     - Request Filtering
   - Performance
     - Static Content Compression (recommended)
   - Management Tools
     - IIS Management Console
     - IIS 6 Management Console (recommended)
     - IIS 6 Management Compatibility
     - IIS 6 metabase Compatibility
     - IIS 6 WMI Compatibility
     - IIS 6 Scripting Tools

8. Ensure all the above Role Services have their checkbox marked, then click **Next**

9. A Summary Screen is shown, click **Install**

Once the install is complete, you may close the Server Manager.

From this point, the standard TMS installer/setup file can be used to install TMS. Follow the normal TMS installation instructions to complete the TMS installation. However, TMS will not function properly until the Windows Firewall has been modified.

The default Windows Firewall Rules will interfere with TMS's communications and is enabled by default on Windows Server 2008. Administrators can choose to disable Windows Firewall or configure the ports required for TMS to be opened. The full list of ports used by TMS is listed below and must be enabled in the Windows Firewall. Not all services will be used in all installations and will vary on the configuration of TMS and the devices to be used. Please see the TMS Product Support document for port specifics per managed device.

Service	Protocol	Port	Direction (relative to TMS)	
			In	Out
HTTP	TCP	80	X	X
HTTPS	TCP	433	X	X
Telnet	TCP	23		X
Telnet Chal.	TCP	57		X
Telnet PLCM	TCP	24		X
FTP	TCP	20, 21		X
SNMP	UDP	161	X	X
SNMP Traps	UDP	162	X	X
SMTP	TCP	25		X
LDAP	TCP	389	X	X
LDAPS	TCP	636	X	X
TMS-Agent	TCP	8989	X	X
Polycom GAB	TCP	3361	X	
Polycom	TCP	3601		X
Polycom	TCP	5001		X

The Windows Firewall for Windows 2008 offers greater controls and profiles compared to Windows 2003. Details on managing the firewall are outside the scope of this document. See http://technet.microsoft.com/en-us/library/cc748991.aspx for documentation from Microsoft for configuring Firewall rules.

Restricting IIS 7 Modules to minimal required (Optional)

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

To modify which modules are enabled in IIS 7

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

   The list of installed Managed and Native Modules are listed. Modules that are not needed may be removed by clicking on them, and then clicking the Remove action from the Action Panel on the right.

The following lists the modules that are **required** for TMS operation and should **not** be removed

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