TANDBERG MANAGEMENT SUITE 8

User Manual

Contents

Introduction

The TANDBERG Management Suite (TMS) is a common portal for carrying out key operations and monitoring your videoconferencing network, including support for TANDBERG and other manufacturer's systems from a central location.

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

The TANDBERG Management Suite lets you easily manage all your TANDBERG systems, including remote software updates and centralized directories.

The TANDBERG Management Suite is web-based, and can therefore be accessed from any workstation running a web-browser. Microsoft Internet Explorer 5.5 and higher is required. 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 tasks such as software upgrading, call control, managing directories and monitoring.

Installation

This chapter gives an overview of the TMS installation. The following components will be presented.

• Installing Internet Information Service (IIS)
• SQL Server installation
• Installing TANDBERG Management Suite

Installing Internet Information Service (IIS)

Windows XP or Windows 2000

During the installation the TMS installer will check for an already installed IIS on the server. If this service is not present, TMS will ask for the Windows CD-ROM and install this before the TMS installer continues with the TMS installation. Follow the steps below if you want to install or reinstall this service manually.

1. Choose 'Start' in the start menu, then 'Settings'→ 'Control Panel'.
2. Double-click Add/Remove Programs.
3. Click Add/Remove Windows Components. This opens the Windows Components Wizard.
4. In the Components list, select Internet Information Service (IIS) and click 'Next'.
5. Click 'Finish' to close the wizard.

SQL Server installation

TMS requires its database to be stored on an SQL server. If no SQL server is installed on the server, the TMS installation will automatically install MSDE 2000. It is also possible to install the TMS database on MSDE 7.0, SQL Server 7.0 or SQL 2000 server. The installation of TMS will automatically detect the presence of any of these on the server and use them when installing TMS.

Installing TANDBERG Management Suite

Hardware Requirements

Pentium compatible processor: 1 GHz or higher.
Memory: 256 MB RAM or higher.

Note: If you plan to manage more than 50 systems with your TMS installation, it is recommended to use a server with minimum 512 MB RAM.

Before installing

Before installing the TANDBERG Management Suite make sure to have the required software installed:

Windows 2000 or Windows 2000 Server

- Internet Information Service (IIS)
- Microsoft Windows 2000 Service Pack 3 or later

In a run-time environment, TANDBERG recommends installing TMS on a Windows 2000 Server operating system, as Windows 2000 Professional only allows up to 5 concurrent web connections.

Windows XP

- Internet Information Service (IIS)
- Microsoft Windows XP Service Pack 1 or later

Their respective companies own all trademarks mentioned in this document.

The Installation

Before you start the installation make sure that you have administrator user rights and that you have your Windows XP/2000 CD-ROM available, as TMS may require to install some Windows components.

1.   Close all open applications and disable virus-scanning software.

2.   Insert the TANDBERG Management 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.   Click the **'TANDBERG Management Suite'** software link.

4.   The installer will search for a previous installed TMS. If a TMS is present, the installer will start an uninstall wizard. By default only the TMS files will be removed and the TMS database will still remain on the server.

5.   The TANDBERG installer will prepare for the installation wizard..

6.   A welcome window will appear on the screen. Press the **'Next'** button to continue.

.

7.   Select 'I accept the terms in the license agreement', and press **'Yes'**.

8.   Enter the licence key enclosed in the CD-cover or sent to you by TANDBERG. (For the three-system version with the TANDBERG Scheduler option, use the suggested license key). Press **'Next'**.

9.   The TMS installer will automatically suggest fields by detecting the servers settings. The IP address of the TMS server should be static.

The SNMP scan range is the network broadcast address TMS will scan looking for systems automatically. TMS estimates the broadcast address based on the TMS server's IP. Modify this field if required to match your network's configuration. If Broadcast is not supported this field should be left blank.

Enter the IP address of your DNS server in the 'DNS Server Address' field. Contact your LAN administrator for this information. The installer will suggest the server's current DNS setting.

The 'From Mail Address' field is the e-mail address TMS poses as when it sends emails and notifications.
     Example: tms@mycompany.com

In the field 'SMTP Server' you must enter the IP address or DNS of the mail server to be used by TMS.

Press the '**Next'** button after completing all the fields.

Note:The TMS settings can be changed in the 'TMS Configuration' menu under 'Administrative Tools' after the installation.
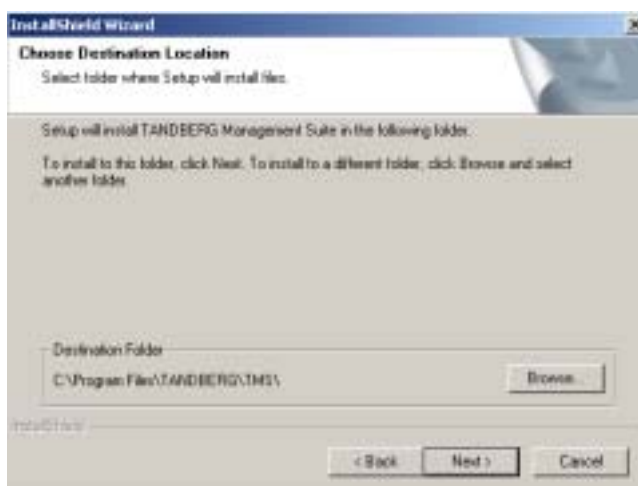
10. This window will appear on the screen only the first time the TMS database is installed.
Fill in the location of the TMS server, and the area code and prefixes. These settings are described in the
chapter 'General Use' - 'Locations'. Press **'Next'**.

11. Press the '**Browse**' button if you want to change the default location where to install TMS,
followed by the '**Next**' button.

12. TMS detects during installation if a compatible MS SQL database already is installed on the server. If one is detected, enter the 'sa' password for this SQL server and press '**Next**'. You will then be asked if you want to take a backup of the existing database before converting it to a format suitable for this release (figure at the bottom of this page). Tick off '**Yes**' if you want to make a backup, and press '**Next**'.

If no SQL server is detected, one will be installed and the entered 'sa' password will be used by this SQL server. Please remember this password for later upgrades of TMS.

Note: to restore the old database, reinstall your old TMS version and use the Database Utility program to attach it to your TMS server. See chapter on Database Backup for further details.
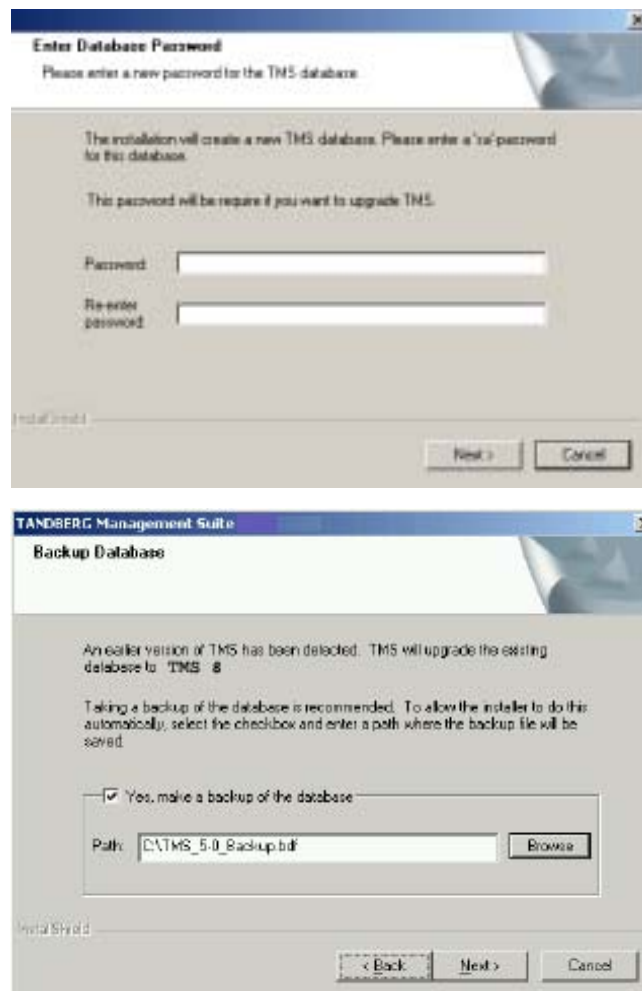
13. Read and confirm the settings displayed in the window, and press the **'Install'** button.

14. The TMS installer will search for an already installed TMS database. If no SQL server or TMS database is installed, the TMS installer will install this automatically. An indicator will show the progress of the installation of the TMS files. To abort the installation press **'Cancel'**.
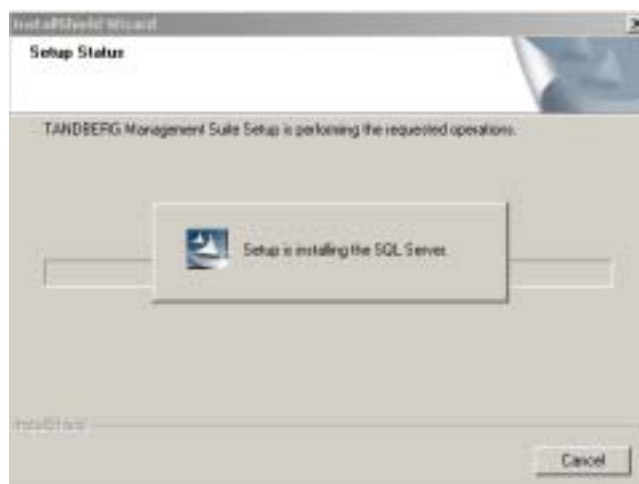
15. Depending on the configurations done by the TMS installer, one of the two screens above will appear on the screen. To finish the installation press **'Finish'**.

Start the TMS program

During the installation the TMS will be added to a program group called TANDBERG. This is located under Programs in the start menu. Select the **'TANDBERG Management Suite'** icon in the TANDBERG folder. To start TMS from another computer, see 'Getting Started' - 'How to start TANDBERG Management Suite'.

Install TMS Network Integration

TANDBERG Provides the TMS Network Integration Plug-In for TMS. This Plug-In enables additional 3rd party support for network infrastructure products such as the Accord MGC MCU range. Please refer to the 'Multivendor Support' section for more information on the level of support provided.

A separate Licence key provided by TANDBERG is needed to enable the TMS Network Integration Plug-In.

Installation

To install the TMS Network Integration Plug-In, double-click on the '**TMSNetworkIntegration.exe**' file which is included on the TMS CD or in the downloaded TMS file package. The following sequence will then follow:

1. A Welcome window will appear on the screen. Press the '**Next**' button to continue.

2. Select 'I accept the terms in the license agreement', and press **'Yes'** to continue.
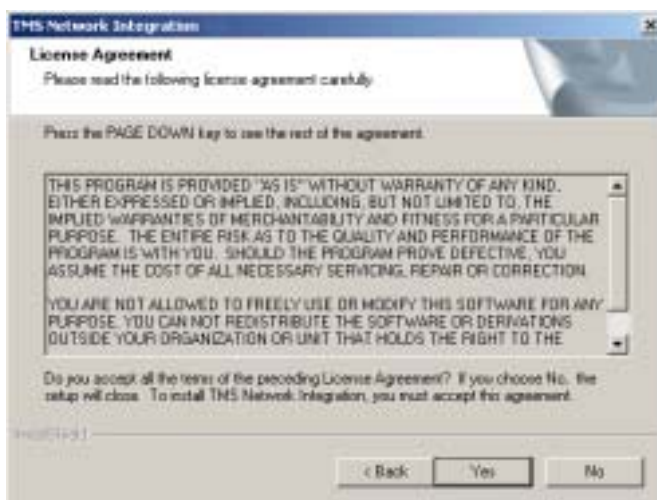
3. Enter the TMS Network Integration licence key enclosed in the CD-cover or sent to you by TANDBERG and press '**Next**'.

4. Verify the information and press '**Next**' to continue.
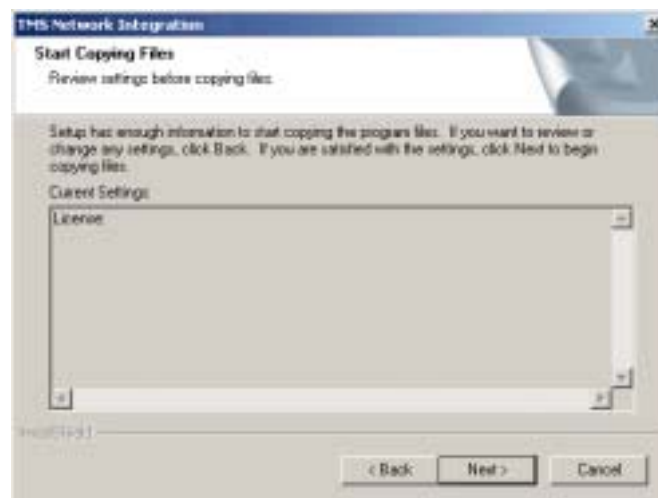
5. When the installation is complete, '**Install Wizard Complete**' will be shown. Press '**Finish**' to complete and exit. Please note that some installations requires system reboot to complete the installation.

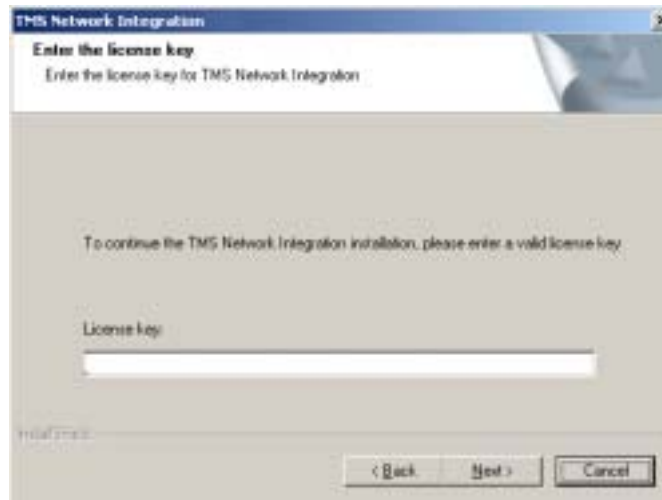Please also refer to the '**Multi Vendor Support in TMS**' for more information.

Uninstalling the TMS Network Integration

To uninstall the TMS Network Integration, start the TMS Network Integration installation component by executing the TMSNetworkIntegration.exe - file. The installation component will then search for the installed Plug-In. When located, the following question will be displayed:
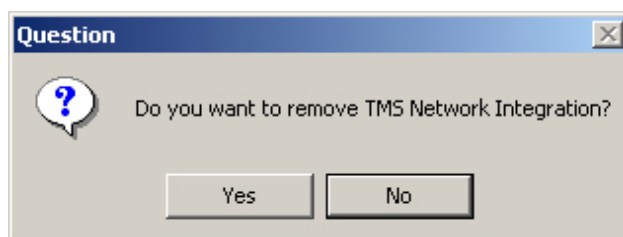
When confirming the deinstallation by pressing the '**Yes**' button, the TMS Network Integration component will be removed. Select if a reboot of the computer should be performed now or later, and then press the '**Finish**' button

Uninstalling the TMS

To uninstall the TMS, select **'Uninstall'** in the TANDBERG-folder from the start menu**.** A welcome window will appear with two options, **'TMS files'** and **'TMS database'**

TMS files

All files used by the TMS will be removed. The TMS database and SQL server will still remain on the server.

TMS database

If this check box is ticked off, the TMS database will be deleted. The database 'sa' password is required for this option.

Upgrade from TMS 5.x, TMS 6.x and TMS 7.x

After downloading the TMS 8 zip file, unzip the file and open the 'Browse.bat' file. If the TMS release has been provided to you on a CD-rom, the 'Browse.bat' file should start automatically.

Following the instructions on the screen to start the installation. The TMS installer will search for an existing TMS database. If a TMS database is present the installation will continue as normal but will automatically import and update all information from the previous installation. You do however need to proide the database 'sa' password in order for TMS to use the installed database.

An indicator will show the installation progress of the TMS files.

Note: If upgrading from a TMS version 6.x or older, you will need a new license key for TMS 7. Please contact your TANDBERG partner for issuing of a new license key.
When upgrading from TMS 5.x to TMS 7, scheduled calls in the database will not be supported (i.e. scheduled calls will be lost).

Upgrade from TMS 4

Due to significant improvements and a large increase of new functions in TMS 8, no upgrade of data from TMS 4 to TMS 8 is supported. If you are upgrading from earlier versions of TMS, the old TMS database will remain intact even after uninstalling. A new TMS database will be created by TMS 8. In order to retrieve data from previous versions of TMS, you must uninstall TMS 8 and reinstall the previous version of TMS.

Registration of TMS 8

In order to receive user-tips and the latest information of new releases from TANDBERG you must register TMS. Follow the steps below to register.

- Click the **'Click To Register'** in the upper left corner of the Portal page of the TMS.

- Press the button **'Register TMS'**

- Fill out the form with your company's information and press **'Register'**. The registration information will be sent to TANDBERG and a registration key will be returned by e-mail.

- Upon receiving the key, click the **'Click to Register'** link.

- Press **'Enter Registration Key'**. Enter the registration key, received by email, and press register. Now your company's name will appear in the upper left corner and you will receive the user-tips and the latest information to the e-mail address you have specified.

Requirements for the TANDBERG videoconferencing systems

TANDBERG Codecs running software version B4.0 or higher benefit from the full functionality of TMS.

TANDBERG Codecs running software version A2 have limited support.

TANDBERG VISION Codecs running doftware version C4.0 have limited support.

TANDBERG codecs with software version earlier than C4.0 are not supported.

For third party product support, please refer to chapter 'Multivendor Support in TMS' in this manual.

Getting started

This chapter will guide you through the main features of the TMS. The areas that are covered are:

- How to start TANDBERG Management Suite
- Fill in your personal information
- Setting up your TMS server
- Adding your first system to a folder
- Book a meeting
- Monitoring systems with Graphical Monitor
- Adding your first TMS Server Phone Book
- Making your first backup of settings on a videoconference system
- Getting your first system statistics

How to start TANDBERG Management Suite
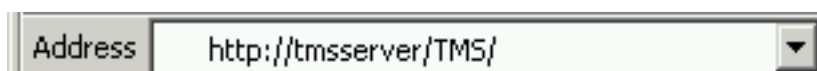
To start TMS, open your web browser and enter the following in the address bar:

http://'*THE IP ADDRESS OF THE TMS SERVER*'/tms

Address   http://10.5.0.25/TMS/

or
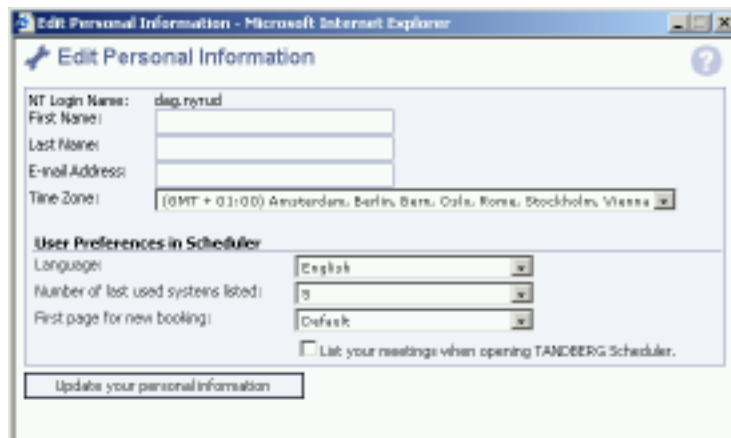
http://*'DNS name'*/tms

Address   http://tmsserver/TMS/

Personal Information

How you login to TMS depends on your Operating System and browser. After entering the URL for TMS, you may be prompted with a Login Window. Login using a valid Username and Password from the Windows Network available to the TMS server.

You may be required to specify the domain name associated with the username. If no domain field is displayed, you may enter it in the username using the format 'domain\username'

The first time any user logs into TMS, they will be prompted to fill in personal information. Fill in all the fields and set the time zone for your location. If your TMS installation includes the TMS Scheduler option, you can also specify the language you want your scheduler to use, how many of the 'last-used-systems' you want listed when scheduling a meeting and tick off whether or not you want to have your meetings as a startpage for TANDBERG Scheduler.

Fill in all the required fields (see figure below), and press the **'Update your personal information'** button.

Note: You can update your Personal information later by clicking on your user name on the top left hand side of the Portal page, or on your name in TANDBERG Scheduler.

Note: The language setting for the TMS Scheduler can be set individually for each user.

Setting up your TMS server

Open 'Administrative tools - TMS Configuration' as shown in the figure.

TMS Configuration

During the installation the most important settings will automatically be set in the TMS server. There are some settings that has to be correct to ensure that the TMS will work properly. Before adding systems or users in TMS, you should go through the following list and ensure that all recommended settings are set accordingly.

1. TMS Default Location (under TMS Settings) - The location given by default to new codecs registred with TMS.
2. SNMP Community Name (under System Interface) - This has to match the community name set on the codec (default: Public).
3. SNMP Trap Host (under System Interface) - The IP-address of the TMS server.
4. DNS Server Address (under Trap Agent Configuration) - The IP-address of the DNS server installed on your network.
5. Watchdog IP Address (under Trap Agent Configuration) - The TMS server IP-address.
6. SMTP Server (under SMTP/Mail Settings) - The DNS name or IP-address of the SMTP server on your network.
7. Web Conferencing (under Web Conference) - URL and passwords to web conferencing servers (if applicable)

Read more about advanced settings in chapter 'Advanced Use - Administrative tools -TMS Configuration'.

Recommended TMS Settings

Before adding new systems and users to TMS, it is recommended that the following settings are considered in order to ease later administration of TMS.

1. In the folder *User Administration* under *Administrative Tools* there is a function called '**Default Groups**'. This is where you define the default access level to new users. In order to control the access level of new users, you should set the default access level accordingly.

2. In the folder *Locations* under *System Management* you can define the different locations that your systems will reside in. In order to ease the process of adding new systems to TMS it is recommended that the locations are predefined before adding the systems.

Adding your first system to a folder

Open 'System Management' - 'Navigator' as shown in the figure.
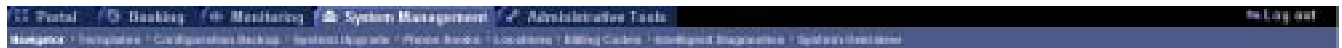
Add Folder

1. Press the **'Add Sub Folder'** button.
2. Type the name of the new folder in the field 'Folder Name' and press the **'Add Folder'** button.
3. The new folder has been added.

Add System

1. Press the **'Add Systems'** button.
2. Type the System IP-Address (or DNS Name) or Check off systems in the list 'Select Systems to Add'.
3. Press the **'Add Systems'** button.
4. If the TMS detects errors in the system settings, a system diagnostic page will be shown.

Text in red indicates errors and yellow text indicates warnings. The TMS will suggest settings to use to set up the systems configurations to match the TMS server settings. Put in the correct settings and press **'Update'**. The New settings will be stored to the system. If you press the **'Skip'** or the **'Skip All'** button the system will still be added to the folder, but this may cause the system not being available for booking and TMS not being able to monitor the system correctly.

5. The system has been added to the folder.

A detailed description of 'Navigator' is given in chapter 'General Use' - 'System Management'.

Book a meeting

To book a meeting select 'Booking - Book a meeting' from the menu as shown in the figure below.

1. Select from the directory or list of systems to be added to the conference. To add a site not listed, enter the Country Code, Area Code, and Number in the fields provided, select ISDN or IP and click the **'Add Video'** button.
2. Press the **'Next >>'** button.
3. Click on a number on the calendar to set the date (to change month, click the **'>'** button on the top of the calendar).
4. Type the starting time in the field 'Starting Time'.
5. Type the duration in the field 'Duration'.
6. Press the **'Next >>'** button.
7. Press the **'Confirm'** button to verify the scheduled call.
8. The call has been scheduled.

A detailed description is given in chapter 'General Use - Advanced Booking'.

Monitoring systems with the Graphical Monitor

To view the Graphical Monitor choose 'Monitoring – Graphical Monitor' from the menu as shown in the figure below.

Graphical Monitor

In Graphical Monitor you can zoom in on all videoconference systems. By clicking a system icon, system information will be displayed. Systems being in a call will be indicated with green lines between them. By clicking a folder, all systems in the folder will be displayed.
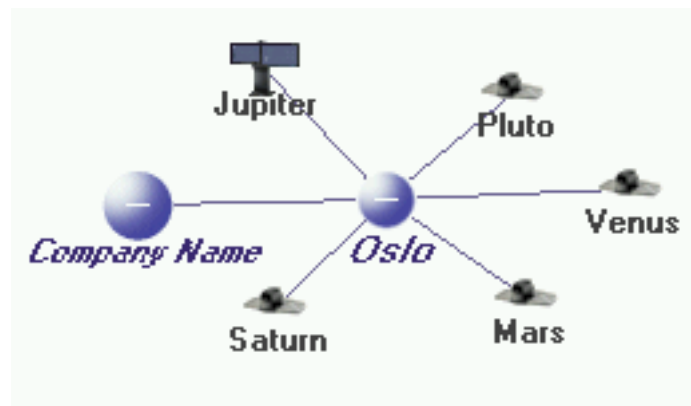
A detailed description is given in chapter 'General Use - Monitoring'.

Adding your first TMS Server Phone Book

A Phone Book is used for saving, organizing and retrieving the names and numbers of frequently called people and/or sites. Names and numbers are stored in the Phone Book and can be retrieved/dialled using the remote control or from TMS.

To create a phone book select 'System Management - Phone Books' from the menu as shown in the figure.

Creating new phone books

Press **'New Phone Book'**. Enter a phone book and press **'Save'**.

Add entries to the Phone book

Click the 'Edit' link to the right of the phone book. Fill in the name, ISDN-number, ISDN-bandwidth, voice-number, IP-address and IP-bandwidth in the fields. Press **'Update Phone Book'** to save the data.

Update systems with Phone books

To load a phone book to a videoconferencing system, click the **'Phone Books'** link on the right of the TMS Phone book. Choose which systems you want to load with the phone book, and press **'OK'**.

A detailed description is given in chapter 'General Use' - 'System Management' - 'Phone Books'.

Making your first backup

To backup one or more system choose 'System Management - Configuration Backup' from the menu as shown in the figure.

Backup settings to TMS

Click on the **'Backup'** link in the menu on the left of the TMS window. Choose the systems to backup by checking them, then press **'Upload to TMS'**.

Restore settings to system

Click on the **'Restore'** link in the menu on the left of the TMS window. Choose the systems to restore by checking them in the list, then press **'Download to Systems Now'**. The backup settings can also be restored to the selected systems every day by pressing **'Daily Download to Systems'** button.

A detailed description is given in chapter 'General Use' - 'System Management' - 'Configuration Backup'.

Viewing your first system statistics

To view statistics select 'Monitoring - Statistics' from the menu as shown in the figure.

The Statistics in TMS will give you detailed information about events and errors on the systems in your network.

The following statistics are available:

Meeting: Call Detail Record (CDR), Endpoint Activity, MCU Activity, Gateway Activity, Billing Codes

Scheduling: Conferences, User, Usage

System: Boot, Authentication Failure, FTP Audit, Low Battery, Trap Log, Connection Error

Network: Connection, Bandwidth, Packet loss

A detailed description is given in chapter 'General Use - Monitoring - Statistics'.

General Use

General use of TANDBERG Management Suite is presented in this chapter. The features of TMS are divided into five main categories.

Portal

This page gives an overview of conferences started from TMS, numbers of systems registered in TMS, diagnostics and TMS user information.

Booking

Use to- book meetings, administrate bookings etc.

Monitoring

Use to- view statistics, graphical monitor, map monitor, event notification and event log.

System Management

Manage the system in the network, includes tools to change settings, backup settings, upgrade systems etc.

Administrative Tools

Use to set up the TMS server, users and groups in TMS Access and view events. Each category above is represented by tabs in the TANDBERG Management Suite menu. Adminisatrative tools are described in the 'Advanced Use' chapter.

Portal

This is the welcome page that will appear on the screen when you start the TMS program. The Portal page gives an overview of Scheduled/Booked conferences, number of systems registered, system diagnostics, TMS user information and system usage measured in percent.
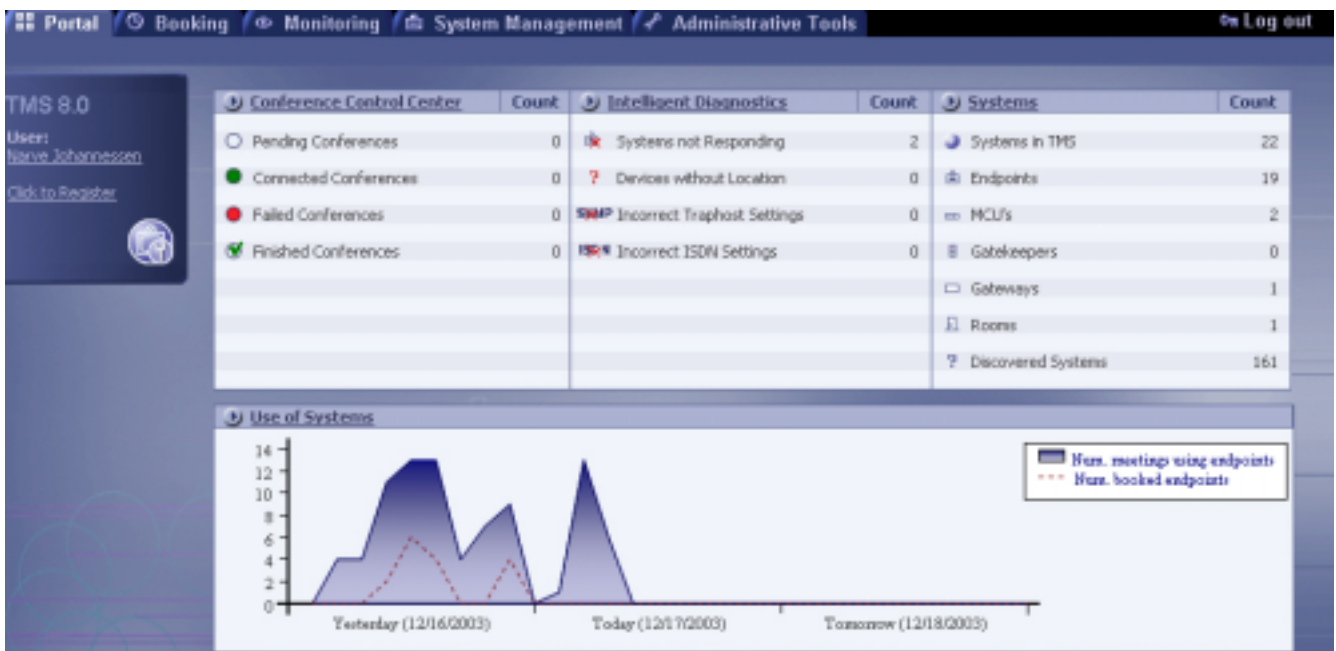
Portal Page of TMS

Booking

The booking feature in TMS gives you the functionality to book rooms and schedule calls.

The Booking tab allows you do book meetings, get an overview of available systems, view your bookings, view all bookings (if you are a site administrator) and start the TANDBERG Scheduler (optional).

When booking a meeting users can set systems to:

- Automatically connect and disconnect at scheduled time.

- Manually connect and autmatically disconnect at scheduled time.

- Manually connect and disconnect (reservation only).

Schedules can be set up from supported systems registered in the TMS to any systems reachable on IP or ISDN.

Book a meeting

To book a meeting the booking wizard is used. There are three steps in the wizard:

1. Select participants

Booking Wizard, step 1: Select participants for the conference.

The participants may be selected from the list of systems registred in TMS. Additional participants not registered in TMS can be added by typing their video or phone number (IP or ISDN) in the fields at the bottom of the page. Press the '**Add Video**' or '**Add Telephone**' button for each number to call to have it registered in the booking. You can also reserve resources for dial-in participants by clicking the '**Add dial In**' button.

If you add more than two systems, be sure that there is a external MCU available or that at least one of the systems has MCU capabilities.

In the 'Settings' window you can specify the 'Call Rate', 'Picture Mode', 'ISDN Restrict', 'Secure Conference' and 'Book for' parameters. These parameters are described below.

Settings

'**Call Rate**' defines the bandwidth for the conference. By default the bandwidth set in the 'Administrative Tools' will be used.

'**Picture Mode**' applies for MCU calls only. Two options are available, Continuous Precence or Voice Switched. By default the picture mode set in the 'Administrative Tools' will be used.

'**ISDN Restrict**' can be ticked off if you want to set up the conference using ISDN 56 kbps instead of 64 kbps..

'**Secure Conference**' can be ticked off if you want to set up a secure conference. All endpoints must support DES/AES encryption. If an external MCU is used this must also have encryption capabilities.

'**Book For**' allows you to book a meeting for another user registered in TMS.The user you book for will receive the confirmation e-mail with an attachment to use with Outlook Calendar. Note that this feature is only available for 'site admin' users.

Press **'Next'** to move to the next step in the booking process.

Note: For booking a meeting with web or data conferencing, please refer to chapter on 'Web Conferencing'.

2. Set the booking date and time.

Booking Wizard, step2: Select start and length for the conference.

Select the date and time for the scheduled meeting. The **'Arrow'** - buttons (**'<'** and **'>'**) above the calendar are used to change the calendar month. TMS will tell you if any other users have booked meetings with any of the systems you have selected.

Reservation recurrence may be selected if the user wants to set up recursive meetings.The options are daily, weekly or monthly. The period for this recursive booking may be set in **'End by date dd-mm-yyyy'**, or the user may set a fixed number of occurences in the **'End after X occurences'**.

Press the **'Next >>'** button when date and time is selected, or press**'Call Now'** to start the conference immediately.

3. Confirmation

Booking Wizard, step3: Confirmation of Scheduled conference, and email notification to participants.

The '**Resevation Type**' can be selected from the scroll down menu, offering the following options:

> Automatic Call Launch: The connection will happen automatically at the specified time and date.

> Manual Call Launch: At the specified time and date, the system listed as the VC-Master will be prompted to begin the call. The call will begin when the VC-Master initiates the call.

> Reservation Only: This selection will reserve the room(s) and will not initiate any connections.

The '**Meeting Password**' field allows the user to password-protect their conference. Any participant wishing to join the conference, then needs to enter this password before joining the conference. The password will be included in the email confirmation sent to the user making the reservation.

The meeting can also be given a title by editing the '**Meeting Title**' field.

Note: If billing codes are required to make a booking (see Administrative tools), a text box for entering the billing code will be presented on this page.

By ticking off the check box '**Display option to extend meeting on VC master**', the VC master will be presented with an option to extend the meeting using the quick keys on his remote control. This option will only be possible if all the resources used in the conference are available for an extension of the meeting.

Clicking on the '**Specify Call Route**' button allows the user to specify how the call will be set up. TMS may give several options for the video conference routing. The user may select which system itshould be called from. If both ISDN and IP are available, the user may select whichever network they prefer. A detailed description is given in the chapter 'Advanced Use' - 'TMS Routing'.

The '**Distributed Call**' check box can be ticked off if you want the call to connect using muliple MCU's in situations where the call is not able to connect using only one MCU. NB! This may lead to reduced videoconference quality

Press the '**Confirm**' button if the data in the list containing scheduling information is correct. (Otherwise choose '**Previous**' and alter the information)

A confirmation email will be sent when the booking is confirmed. You have to be registered with a valid email address (e.g. me@mydomain.com) in TMS to be able to receive a confirmation e-mail of your TMS booking.If you would like several participants to get an email confirmation for the meeting, feel free to fill in any email address in the **'To: '** field. If you fill in several addresses, seperate the addresses with a **';'** sign.

Note: The confirmation e-mail provides the meeting details, and an attachment that will generate an appointment in your Outlook Calendar with a reminder 15 minutes before the meeting.

FreeBusy Overview

The 'FreeBusy Overview' folder under 'Booking' displays an overview of reservations and available systems at a given point in time. This is an excellent tool for quickly verifying the availability of systems and ad hoc conferences.

FreeBusy Overview

To get the latest free/busy information enter a date, start time and duration and then click the '**Query**' button. The black bars in the FreeBusy Overview screen indicates the time-span you defined in your query.

From the folder structure on the left side of the screen, you can select the system or room you wish to book. It is also possible to add external dial-in participants and enable data conferencing (if available) at the bottom of the page.

To book one or more systems, first enter a date, start time and duration at the top of the page, then selected one or more systems. Finally select either the '**Reservation Only**' button to reserve those specified systems or room at the selected time or the "**Automatic Call Launch**" button to start and end calls automatically at selected time.

If you select the "**Automatic Call Launch**" button a pop-up window will appear displaying the call route between the meeting participants. TMS will also send a confirmation message to your email address, containing an Microsoft Outlook attachment that can be double-clicked to update the Outlook calandar. If data conferencing has been selected, the mail will contain a web-link to the data conference (optional).

My Meetings
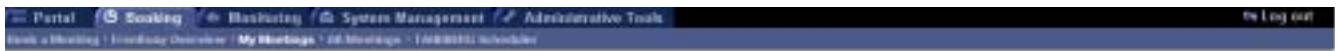
The 'My Meetings' folder gives an overview of the users meetings. By default only meetings currently active or meetings that are scheduled to take place in the future are listed. The user may select to view this week's meetings, this month's meetings or all meetings booked by the user.

To view previously held meetings, select the '**Old Meetings**' button. The old meetings will then be listed below the ones not yet completed.

The table gives an overview of the meeting type, date, start time, duration the meeting was booked for, Meeting id, title and number of rooms. For 'old meetings' you also get the list of participants.

A set of icons are shown on the right-hand side of each meeting representation. These icons have the following meaning:

Press ![i] - to view meeting datails and status

Press ![x] - to delete the meeting

Press ![edit] - to edit the meeting

Press ![end] - to end the meeting. This will disconnect the conference if it is connected.

Note: You can use an old meeting as a template for a new one by editing the old meeting and changing the start time for the meeting (as well as other paramters if needed).

You can also view details about an ongoing or scheduled meeting by clicking on it. The meeting information will then be displayed on the bottom half of the screen.

Here you will find detailed information about the meeting, including participant information, date and time, bandwidth usage etc. You can also view the dial list and dial events by pressing the '**View Dial List**' and the '**Dial Event**' buttons, respectivley. You can also do changes to the meeting, by adding or removing participants and adjusting the time settings for the meeting.

Note: in order to get a web snapshot of the conference, both endpoints must have Web Snapshot enabled, and the call can not be secure (encrypted).

All Meetings
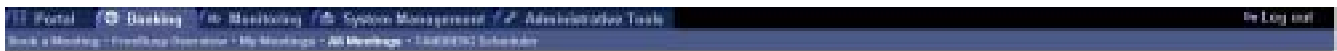
The 'All Meetings' feature is only available for TMS users with administrative rights. It gives an overview of all meetings booked in TMS.
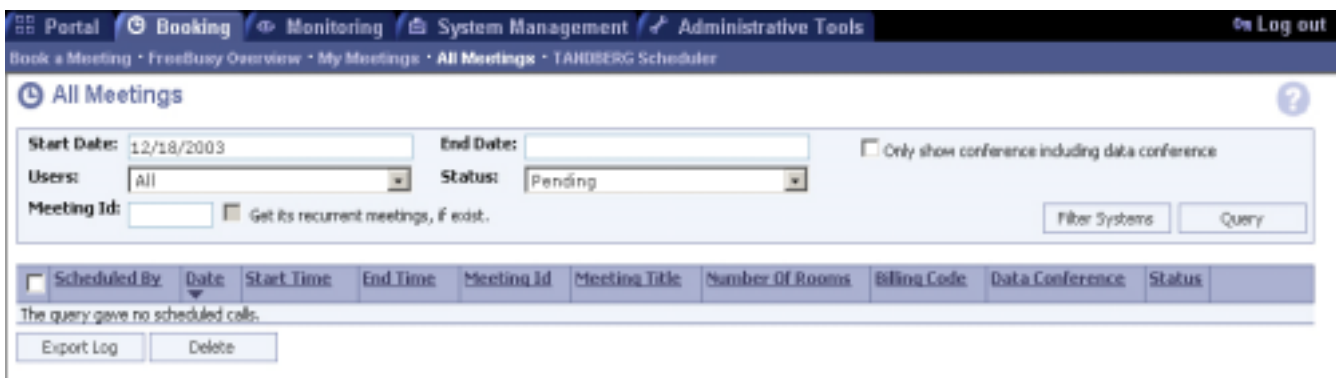
There are numberous filtering mechanisms available for the TMS administrator to narrow down the presented list of meetings. These include

*   Date (Start and End Date): Enter dates in respective fields.

*   Users: Select meetings booked by specific users by using the scroll bar, or select 'All'

*   Meeting ID: Enter the meeting ID

*   Status: Select which call status you want presented by selecting from the scroll-down menu. Options here include: All, Pending, Pending an Ongoing, Ongoing, Finished, Meeting Request and Rejected.

*   Data conferences: Checkbox to display only conferences including data conferences.

*   Systems: Press the '**Filter Systems**' button to view meeting involving specific end points or MCUs.

Having set all the wanted filtering paramters, press the '**Query**' button to execute the query.

The list can be printed or stored for later use, by pressing the **'Export Log'** button. A CSV file will be generated, this file can be opened in MS Excel.

From the 'All Meetings' page you can also edit and delete scheduled calls.

To edit a booked meeting press the edit-link. Booked meetings can be deleted by checking the calls to be

TANDBERG Scheduler

The TANDBERG Scheduler is an (optional) tool for easy scheduling of conferences. The tool offers simple to use scheduling mechanisms, reducing the complexity of booking conferences to a minimum.

The TANDBERG Scheduler has multilingual support, enabling each individual user to have the TANDBERG Scheduler presented in his language of choice. Languages supported by the TANDBERG Scheduler are:

English	German	French	Italian	Russian
Norwegian	New Norwegian	Swedish	Spanish	Portugese
Japanese	Korean	Chinese (simplified)		

The TANDBERG Scheduler has extensive on-line help support, and is so easy to use that no specific user manual should be needed.

The TANDBERG Scheduler

Monitoring

In the Monitoring folder you will find several useful tools to monitor the systems controlled by TMS, view statistics and events.

The Conference Control Center, Graphical Monitor, Map Monitor, Statistics, Event Notification and Event Log-folders will be explained in the following chapters.

Conference Control Center

With the Conference Control Center, you can get an overview of all conferences booked either using 'Advanced Booking' or using the 'TANDBERG Scheduler'. Please note that you can narrow down or expand the displayed list of conferences by ticking off the filter check-boxes for the conferences of interest (e.g. pending conferences, failed conferences etc.). You can also filter the conferences displayed by setting the 'From Date' and 'To Date' fields. If the Conference Id is known, this can also be entered in the '**Id**' - field to go directly to the desired conference.

ConferenceControl Center

By clicking on a displayed conference you will get information about the booked meeting in a separate pop-up window.

Conference Details

This Conference pop-up window gives you a complete overview of the conference, the participants, bandwidth usage, time, duration etc. Clicking on the participant listed, you can view and set the settings of the selected system. You can also add participants to the conference, you can remove participants from the conference, adjust the time for the conference as well as ending the conference.

You can also view the dial list, the dial events and the disconnect events (for ended conferences).

Note: If there is a web- or data-conferece used in the conference (which is booked using TMS), you can also join the web conference from the Conference Control Center.

Information for all conferences

Id: The meeting-id for the conference. This number will increment with one for each booked/ scheduled meeting.

Title: The name of the conference specified in the Booking/Scheduling wizard.

Type: Type of call - how the call was set up.

Owner: The name of the owner of the conference (not necessarily the person who booked the meeting)

Master: The master of the conference, specified in the Booking/Scheduling wizard.

Bandwidth: The Bandwidth specified in the Booking/Scheduling wizard.

Date: The date of the meeting.

Start Time: The start time of the meeting.

End Time: The end time of the meeting.

Duration: How long the meeting has lasted.

Time Left: The remaining time before the meeting is disconnected.

Secure: If the conference is secure or not.

Video IP: Number of IP Video calls in the meeting.

Video ISDN: Number of ISDN Video calls in the meeting.

Telephone IP: Number of IP-Audio calls in the meeting.

Telephone ISDN:Number of ISDN Audio calls in the meeting.

Password: The password required to participate in the meeting.

Picture Mode: The picture layout selected for the meeting.

Participants: Lists the participants of the conference.

ApproveMeeting

If meetings booked by users must be approved by the TMS administrator (an option that can be set under 'Administrative Tool - TMS Configuration'), these will be highlighted in the Conference Control Center. The TMS administrator can approve or reject the meeting by right-clicking on the meeting in the Conference Control Center and select the wanted option.

Graphical Monitor

The TMS Graphical Monitor has powerful features for monitoring a network of conferencing systems, gatekeepers gateways and MCU's. To use the Graphical Monitor choose **'Monitoring'**, then **'Graphical Monitor'** in the menu.

The graphical monitor gives a graphical representation of all the videoconferencing systems in your network.
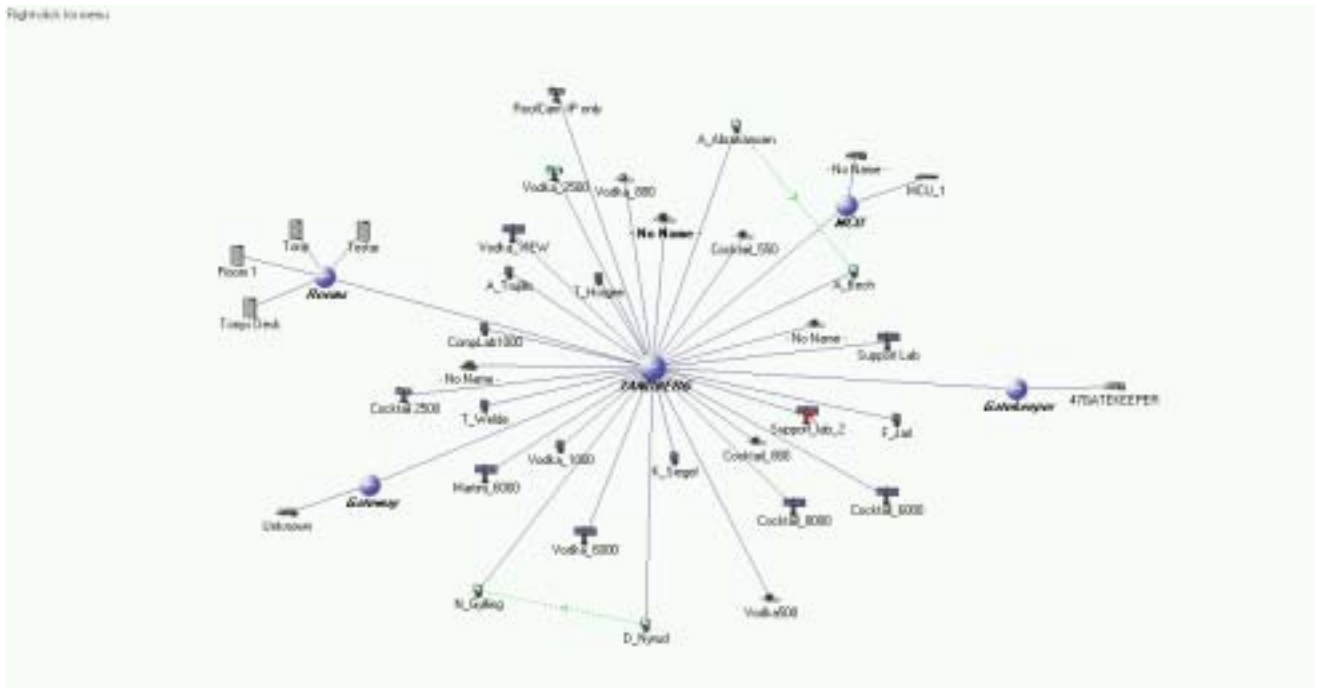
Graphical Monitor

The following chapters will describe the options provided by the Graphical Monitor.

Folders can be opened or closed by double-clicking on their icon, or by right-clicking on the folder and selecting **'Open'** or **'Close'**.

All videoconference systems can be displayed and zoomed in on, by clicking directly on the icon representing the system. When a system is selected, the system information is displayed in a separate window. See chapter 'General Use' - 'System Navigator' for details on using this page.

By right-clicking in an empty space on the Graphical Monitor page , a menu is displayed.

Arrange

Selecting 'Arrange' will cause the position of the folders and systems to be arranged automatically for best fit in the graphical monitor.

Expand All

Selecting 'Expand All' will cause all sub-folders to be expanded and displayed on the Graphical Monitor.

Show Control Panel

With the Control Panel you can choose between different presentation options.
For example it is possible to show only systems with status 'No response',
or only systems currently in a videoconference.

Zoom (scrollbar)

When the bar is moved to the right, the length of the edges between folders and systems are increased. When the bar is moved to the left, the length of the edges aredecreased.

In Call (checkbox)
If this checkbox is checked, systems that are in a call are shown.

No Response (checkbox)

If this box is checked, systems with status 'No response' are shown.
Systems that are turned off, not connected to the network, or with some
kind of network problem will be visible.

Idle / Alive

If this is checked, systems that are alive or idle will be shown in the monitor.

Show Info Frame

By selecting 'Show Info Frame', the bottom half of the screen will be used for displaying information about each
system representation in the Graphical Monitor.

Options

By selecting 'Options' you can change the user settings of the Graphical Monitor.

Show Name

The system name will be shown for all systems in the graphical monitor.

Show IP Address

The system IP adresses will be shown for all systems in the graphical monitor.

Visible Characters

Allows you to choose how many characters will be displayed for each system.

Font Size

Choose between 'Normal', 'Large' or 'Very Large' font size.

Label Color

Choose between 'Black', 'Blue' or 'Red' coloring of the label text for each system.

Animation

The speed of the animation of systems in call. This animation is shown as circles around the systems in call with systems not registered in the TMS. You can choose between 'Fast', 'Normal' or 'Slow'

Update Frequency

The update rate of the graphical monitor in seconds, when checking system status of each system. Choose within an interval from five to sixty seconds.

Show Call Animation

Turns the animation of the systems in a call, on or off. Note: Using animation requires more resources from the TMS-client.

Show Call Lines

Turns the lines drawn between systems registered in TMS who are in a call together on/off

Auto Arrange

If this is enabled TMS will automatic arrange the folders and systems in the graphical monitor.

Map Monitor

The TMS Map Monitor is designed to give an overview of the physical locations of the systems in your network. Each folder can be associated with an own background picture (e.g. country map, map of an office building etc.) where the conferencing systems are placed on the picture. The Map Monitor is found under 'Monitoring' and 'Map Monitor'.

Set up an organization in Map Monitor

Only the administrator in TMS can organize conferencing systems. Other users can see the systems on the map, but cannot create/delete folders, move systems between folders or place the systems on the background pictures.

In order for the Map Monitor to be used efficiently, the folders created in TMS should correspond to the physical location of the conference systems. The folder hierarchy is designed to make this as easy and efficient as possible.

E.g. a conference system in an international company 'MyCompany' located in Chicago should have a tree structure corresponding to: MyCompany/ MyCompanyUS/ MyCompanyChicago. The three folders should be associated with one background picture each. Suitable background pictures to be associated with the three folders would be: a world map, a US map, and a layout map of the office in Chicago. The lay out map would show all the rooms in the Chicago office, and the icons for each conference system would be placed in the right room.

The figure illustrates the folder 'MyCompany', located in USA. This folder is placed on the world map.

The figure illustrates the the company`s office in Chicago. The folder icon is placed in Chicago.
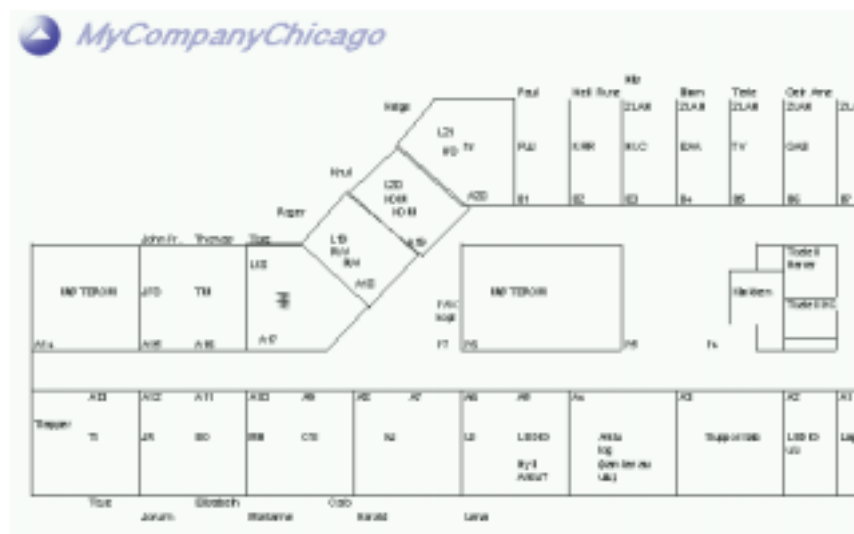
The figure illustrates the office building in Chicago. The system icons can be placed in their respective offices.

Organizing folders and Icons in the Map Monitor

In order to move a conference system or a folder, simply drag the icon by holding down the left mouse button and release the mouse button to place the icon. If the conference system should be moved in to another folder, just drop the icon on the folder. To move a system upwards in the folder hierarchy, drag and drop the system to the icon (blue circle with white triangle) located in the upper left corner of the map window. The folder structure is the same as in the rest of TMS, and any changes in the folder hierarchy or movement of conferencing systems is automatically updated in the TMS.

Background Images

Every folder can be assigned its own background image. To change the background image, simply click the right mouse button in the window, and select 'Change Background Image', see figure below.

In this view a default background picture can be selected, or you can upload a background picture of your own by clicking the 'Upload New Image' button.

SELECT BACKGROUND IMAGES.
The background picture must be in the GIF or a JPG format, and a size between 400x400 and 1000x1000 pixels is suitable.

Control Panel

See chapter 'TMS Graphical Monitor' - 'Set up your Monitor' for information on the functionality of the Control Panel. In addition to the functionality described in the chapter, the Control Panel has a **'Grey Map'** feature. The feature makes the maps used as background images grey; this to enhanced the contrast between the systems (which are still in color) and the background.

System icons

Idle System Icons

The System icons are used both in the graphical and the map monitor.There are four different system icons: Set-Top icon (T500, T550, T800, T880), Table-Top icon (T1000), Meeting System icon (T2500, T5000), Conference System icon (T6000, T7000, T8000), Network component icon (TANDBERG MCU and TANDBERG Gateway). In addition, selected 3rd party products have their own icons.

In Call System Icons

If a videoconference system is in a call, the system icon changes. The Set-Top icon gets a green dot in the camera. The Table-Top, Meeting System and Videoconference System icon get green screens. The TANDBERG MCU get green dots in the front panel. This is done to graphically show that the system is in call. If the call is encrypted, there will also be a small padlock 🔒 down to the right of the system icon. A system that is in a call with a system not registered in TMS will have a flashing circle around the icon. Selected 3rd party products will also have green screens to indicate that they are in a call.

No Response System Icons

If a system has status 'No response', the system is marked with a red cross. ✗

Unknown Devices

Unknown end points are shown with a questionmark. ?

Statistics

TMS Statistics are used for logging activity on registered systems. To view the system statistics select **'Monitoring'** and then **'Statistics'** from the main menu. 'Endpoint Call Activity' is then shown as default.
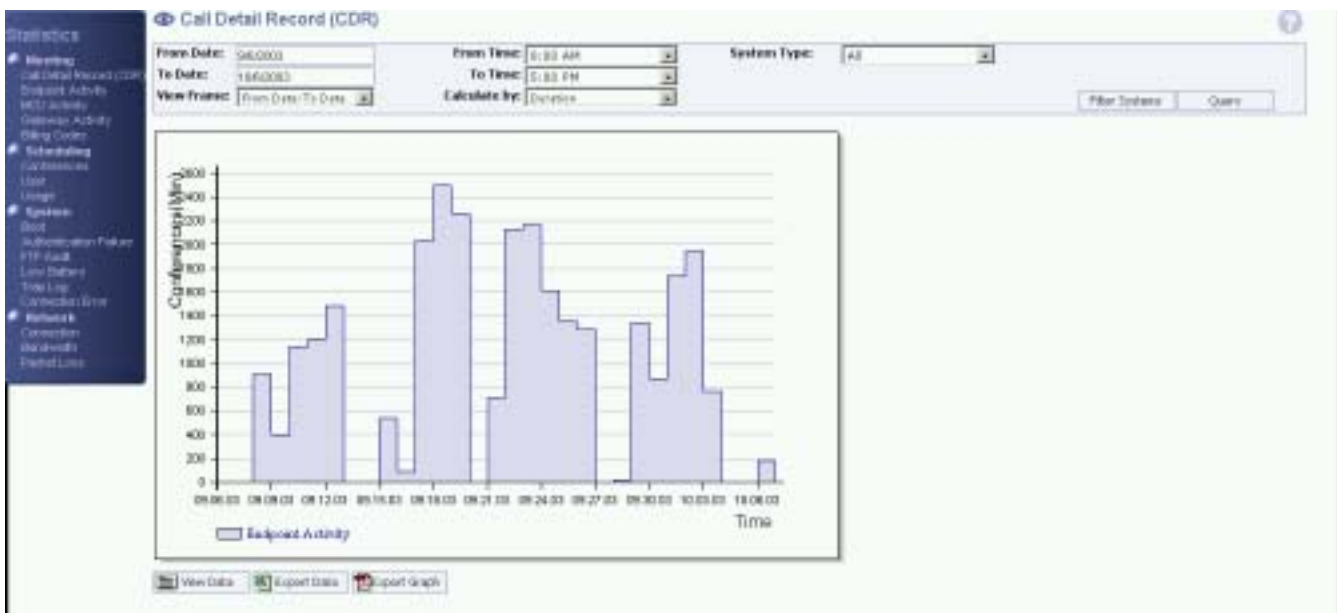
Statistics overview.

Note: *To export statistical data to an Microsoft Excel sheet or in pdf format, the TMS server needs the required MS Office and Adobe Acrobat components installed. If these components are not installed, the exported data will be presented in csv format (Comma Separated Values).*

Filter System

The '**Filter System**' button makes it possible for the user to view statistics for specific endpoints.

Date and Time

You can select the time interval (date and time) for which you want statistics presented. Enter the date- and time-range in the corresponding fields on the statistical page and select the '**Query**' button.

TMS offers a full range of statistical data. These are grouped in to 4 different categories, listed on the left-hand side of the Statistics page: Meeting, Scheduling, System and Network. More details about the statistical content of these groups can be found below.

All statistical data can be exported into varying formats, depending on the type of statistics in question. Icons representing the possible export options are displayed at the bottom of each page presenting statistical data. Options here include Excel spreadsheet, PDF formats or CSV (Comma Separated Values).

Meeting

'**Call Detail Record**' offers the possibility to view and export Call Detail Records (CDR) for endpoints, MCU's and Gateways in your network. Data can be collected for defined time intervals on selected systems. The CDRs contains all required information in order to charge end-users for their usage of bandwidth and network resources, including billing codes, numbers dialled, protocols and duration.

'**Endpoint Activity**' gives an overview of end point activity for the filtered systems (all by default) for the defined time period. If you click on the bargraph to a selected endpoint, the number of calls made on the system in a certain time interval will be shown. Click on the '**View Data**' button to see more information about time of occurrence, call direction, remote site, duration, protocol, bandwidth, call type, cause code and billing codes used for all the calls plced by this endpoint.

'**MCU Activity**' gives an overview for the filtered MCU (all by defualt) for the defined time period. If you click on the bargraph to a selected MCU, the number of calls made using that MU in a certain time interval will be shown. Click on the '**View Data**' button to see more detailed information about the activites on this MCU.

'**Gateway Activity**' gives an overview for the filtered gateways (all by defualt) for the defined time period. If you click on the bargraph to a selected gateway, the number of calls made using that gateway in a certain time interval will be shown. Click on the '**View Data**' button to see more detailed information about the activites on this gateway.

'**Billing Codes**' gives a bargraph for all billing codes used in a conference setup.

Scheduling

'**Conferences**' displays time and number of scheduled conferences made in TMS in a time interval. Click on 'View Data' to see more detailed information about the scheduled conferences having taken place.

'**User**' displays how much each user schedules. Statistics are shown for bookings taken place with either er using TMS Booking, TMS Scheduler or other scheduling tools. In the upper right hand corner there's a graph representing the percentage usage split between these three scheduling methods.

'**Usage**' displays more detailed statistical information about the usage of the TANDBERG Scheduler.

System

'**Boot**' gives statistics for all boot events on systems registered in TMS.

'**Authentication Failure**' gives information over all failed login attempts on systems that require a password when accessing the systems by Telnet, FTP, HTTP or SNMP.

'**FTP Audit**' gives an overview of all FTP (File Transfer Protocol) activites towards a system. Requires TANDBERG codec version B7.2/E2.2 or later, TANDBERG MCU version D3 or later and TANDBERG Gateway version G2 or later.

'**Low Battery**' tab displays the number of low battery events on endpoints remote control in a specified time interval.

'**Trap Log**' gives a detailed log that describes all the events that are registered in a particular system. This log reports reports events like scheduling, errors, encryption status etc.

'**Connection Error**' gives a detailed log that describes connection errors only. This log reports an error with a cause code. Useful information to determine if there are network problems to a system.

Network
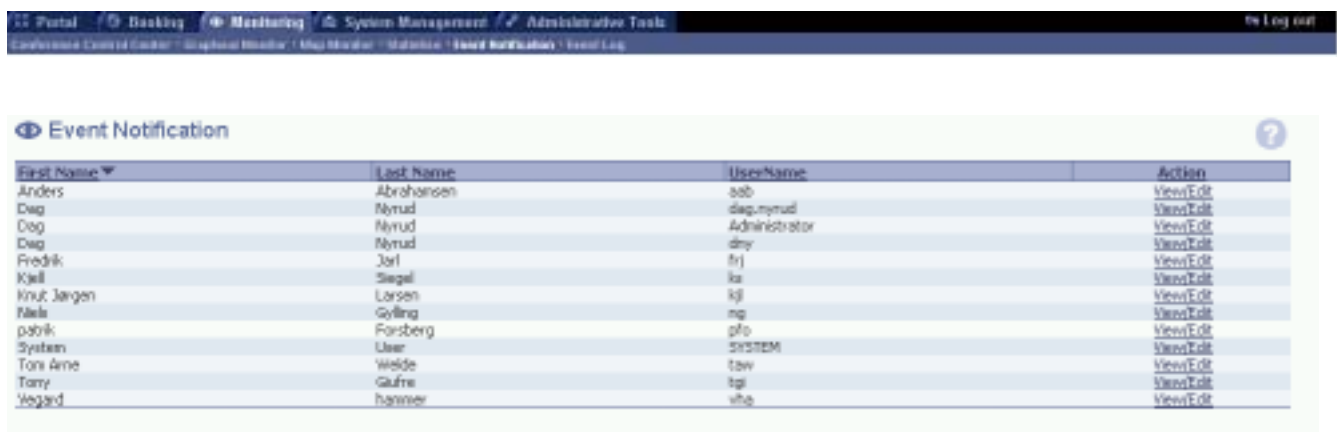
'**Connection**' displays all connection attempts for a system. Information like Got Response, Lost Response, Link Up and Link Down is typical events that will be reported.

'**Bandwidth**' displays a graph showing the average use of bandwidth within a time period for a selected system, measured in Kb/s.

'**Packet Loss**' displays a graph showing the percentwise packet loss (IP packets) for all the connections in a given time period.

Event Notification

To open the 'Event Notification' tool, select **'Monitoring'** and then **'Event Notification'** from the main menu.

The event notification module gives the functionality to subscribe to events, and be notified by email whenever the event occurs. Users in TMS can subscribe to events they have access rights to. One can e.g. register to be notified by email every time a certain system is connected.

To use the event notification wizard in TMS follow these two steps:

• Select user for whom to set a certain event notification level.

• Select system(s) and events to be notified on. The selected events will be sent by e-mail to the user.

Event notification.

From the Event Notification menu select the systems to monitor. Note that access to events is based upon the group a user belongs to. The administrator must give the user's group permission to that event, otherwise the event will not be listed.

Select events to notify.

In the Event Notification Menu select the system to monitor, and the tick off events to be notified on.Press the '**Add'** button. Information about the selected systems and events are displayed in field C to the right on the screen.

Event Log

The event log is accessible under the Monitoring tab.

In the Event Log the user is able to get information about events for all systems registered in TMS. Use the filter button to choose time interval, and from the list select desired event to read. Available events are:

- All Events
- Dial Events
- Directory Events
- Disconnect Events
- Display Text Events
- Upgrade Events
- Conf. Backup Events
- Conf. Restore Events

By selecting one event, you get a pop-up window describing in more detail what happened.

System Management

In the System Management folder you will find powerful tools for managing videoconferencing systems connected to your network. Systems can be added and deleted from TMS, grouped and organized in a tree-structure.
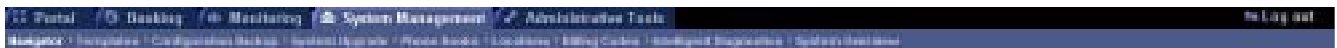
The different folders Navigator, Templates, Configuration Backup, System Upgrade, Phone books, Locations, Billing Codes, Intelligent Diagnostics and System Overview under the System Management folder will be described in the following chapters.

Navigator

The System Navigator is a powerful tool to get an overview of systems registered in TMS. This is also were an administrator can sett group access levels to the different systems (See also 'User Administration' under 'Advanced Use'). The Navigator allows for several different views, which are selectable from the pull-down meny on the Navigator. It is however only under the 'Folder' view that group access control for the systems can be defined.

In the Navigator, you can expand and close folders by clicking on the '+' and '-' symbols respectively. If you click on a folder name, all the systems organised under this folder will be listed in the right-hand window.

Folder View

The Folder view allows you to organize your videoconferencing systems in a tree structure, which gives intuitive navigation and easier localization of the systems. Navigator includes adding and removing of folders and systems, and setting access rights. A system can reside in several folders. By clicking on a system, either in the main window or in the left menu, information and settings for that system is displayed.
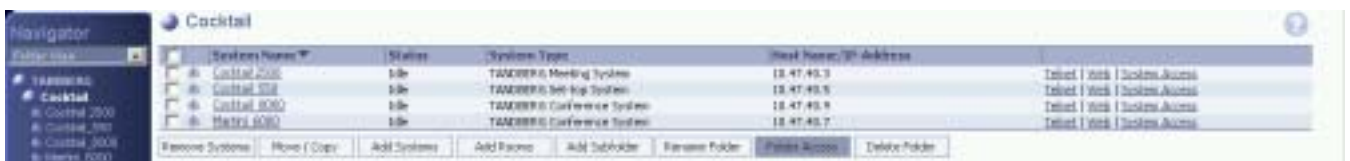
The Navigator

By selecting the '**System Access**' link to the far right of each system, you will be able to set access rules to the specific systems. Please see chapter on 'Folder Access' (later in this chapter) for a description of the different access levels that can be assigned to both folders and systems.

A short description of the buttons:

Remove System

Removes the checked systems from the folder. The user can choose to remove the system completely from the TMS server, or just remove it from the current folder in the system tree structure.

Move/Copy

The checked systems are moved or copied to other folder(s).

Add Systems

Allows a user to add systems by entering an IP-address or DNS-name, scan for systems within an IP-range, add a system without SNMP support (currently only Polycom ViaVideo) or select systems already registered in TMS or found during a discovery scan by the watchdog. When adding video conferencing systems to TMS, the following settings will be checked:

- SNMP Traphost IP-address - is set to the value of the TMS server.

- SNMP Community Name - is set to one of the SNMP community names listed in the 'adminstrative tools' page.

- Location - is set to a valid location.

- If the system is set-up to handle ISDN calls (the systems PRI, BRI or external interfaces are active) TMS will check the ISDN base-number of the system with the country set in the location profile.

- If the system is not set-up to handle ISDN calls, and a gateway has been set-up for the location, TMS will check the H323-gatekeeper settings of the system. A H323-gatekeeper must be set in order to use an ISDN gateway.

- If the system is not set-up to handle ISDN calls, and no gateway is set-up to be used for the location, the system will be added to TMS. Only IP-calls will be allowed.

- If TMS finds one of the values to be incorrect you will be asked to correct the setting. You may be asked to update settings on the video conferencing system, so please have the manuals for the systems available.

Add Rooms

Add a new room to the current folder.

Add Sub folder

Add a new folder to the current folder.

Rename Folder

Rename the current folder.

Folder Access

Folder Access allow you to restrict and control the access to folders.

There are defined 4 different access levels to folders and systems. These are: No Access, Book, Monitor, and Admin.

No Access:	The group has no access at all to the folder or systems The folder will not appear in the 'System Navigator' for users belonging to groups with no access.
Book:	The group can see the folder and schedule any systems set to Book.
Monitor:	The group can see the folder and schedule and monitor calls for any systems set to Monitor.
Admin:	The group can use and modify the folder and book, monitor and modify any systems set to Admin

In the same menu, it is possible to tick off whether you want the settings to apply to all systems in the folder in addition to all the sub-folders.

Checking off the **'Apply to systems in folder'** checkbox will update the systems in the current folder.

Checking off the **'Apply to subfolders and systems in subfolders'** will update all the systems in the current folder, and all the systems in its subfolders.

Note: A new group can be created/edited in the TMS User Administration menu. This is described in 'Advanced Use' - 'Administrative Tools' -'User Administration'.

Alternative Navigator views

It is also possible to select other views for presenting the systems defined in TMS. In the Navigator pull-down menu you can in addition to the default '**Folder**' view select to view the systems arranged according to System Type, System Category, Manufacturer, by Location, by Connection Status or by Software version. You can also get a list of all the systems registered in TMS (organized under the same folder) or even search for a system by either system name, IP address, ISDN number, E.164 alias or by Software version.

It should be noted that only systems that a user has access rights to will be presented under the different views provided by the Navigator. Access level is defined under Folder view by an administrator.

Here are some example- views:

By Manufacturer
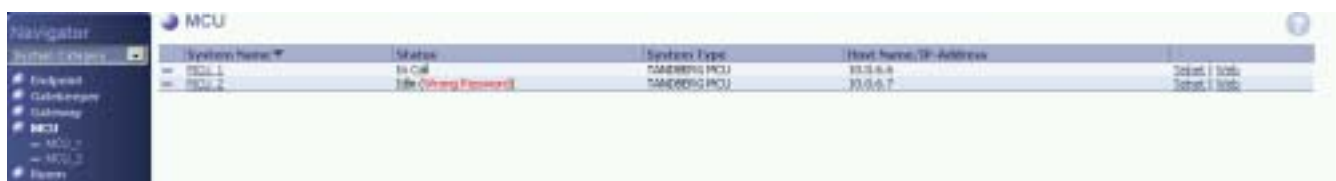
By System Category

Note: you need to select a folder to view the systems in that folder.

System Information

To select a specific system in the System Navigator view, click on a System Name in the tree structure menu on the left, or on one of the systems shown in the current folder.

VIEW OF SYSTEM INFORMATION
Note! Menu selection may vary depending on system type.

General information about the system is shown in this view. Some of the system information can be edited from the 'Intelligent Diagnostics' page of the system. The '**Edit using Diagnostics**' buttom will take you directly to the editing function of the 'Intelligent Diagnostic' page.

You can also force a refresh of the System Information about the system by clicking the '**Force Refresh**' button.

There are three links in the upper left-hand corner offering the following functionality:

•   The **'Web'** link takes the user directly to the web interface of the system.

•   The **'Telnet'** link opens a telnet connection to the system.

•   The '**FTP**' link explore the files and folders on the system using FTP.

Other System Settings

This page shows settings which are specific for this brand of system other than the general settings.

Some of these parameters may be edited. Enter new information into text fields and click on the '**Update**' button to store your changes on the system.

Note! Parameters may vary depending on system type.

Settings

Shows all the system settings. By pressing the **'Backup Settings to TMS'** button, the user may save
these settings on the server. If settings are stored on server, these will be shown together with the
system settings.

Differences between settings on the system and settings stored in TMS will be highlighted for quick configuration
checking. This feature makes it very easy to identify if someone has made a change to the system. If the system
settings have not been stored previously, the right column will be blank and the 'Restore Settings on Systems'
will not be displayed.

To restore settings stored on the TMS server to the system, you need to access the '**Restore**' function under
System Management-Configuration Backup.

Settings on a System

Intelligent Diagnostocs

The Intelligent Diagnostics page shows diagnostics for this system. This diagnostics page gives an overview of the parameter settings of the system, as well as indicating errors on the system and how to correct these.

Different colour codes are used to indicate the severness of the errors. Warnings are written in yellow, while errors are written in red.

Intelligent Diagnostics for a selected system

Phone Book

Displays the directory or phone book of the system. Local directory entries can be edited from this screen along with selecting a server directory. The system will be updated with the new directory shortly after it is selected.
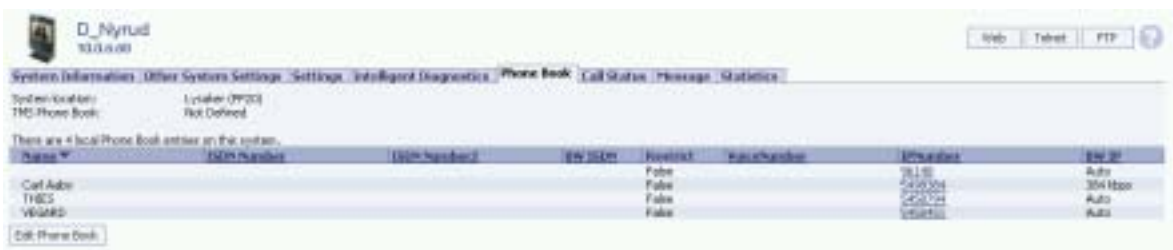
Phone book

Call Status

Displays the current call state of the system. When a system is in a videoconference, information about the connection is shown. It is possible to make a call using the number field and the dial button, and to disconnect with the 'Disconnect' link. The **'Refresh'** button retrieves the latest information from the system**.**

Call Status

Message

Type a message in the 'Message' field, and press **'Send'** to send the message to the system. The message is displayed on the screen of the videoconferencing system. 'Message Duration' allows the user to set how many seconds the message will be displayed.

Message

Statistics

A list of available statistics for the specific system is shown under 'Statistics'. Select which statistics you are interested in. This will take you to the *Monitoring-Statistics* folder, where you can do additional filtering (on date and time) for the selected system. Use the 'Back' button on you browser to return to the list of available statistics for your selected system.

Available statistics are:

- Scheduled Conferences
- System activity
- Boot
- Low battery
- Trap Log
- Connection Error
- Connection
- Bandwidth

Templates
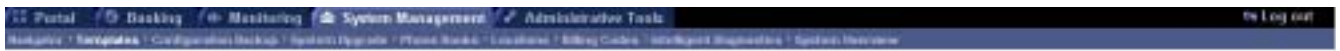
Using templates, the user can download a specific set of settings to several systems in one operation. This ensures homogenous settings among different systems, and TMS makes this operation easy and effective.To view the templates, select 'Templates' under 'System Management'.
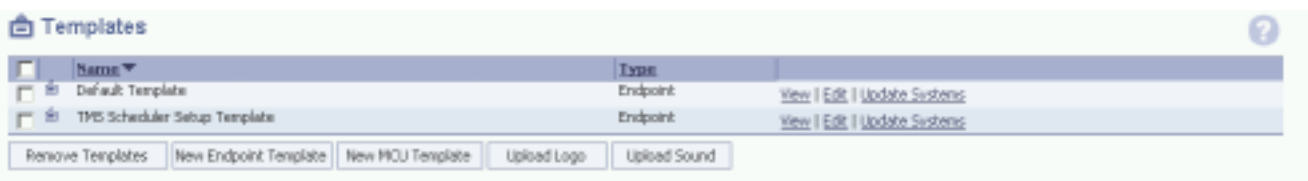
List of templates.

New Endpoint Template

This template is used for TANDBERG endpoints. In the list of available settings, hook off and set the wanted value for all the settings you want to have in the new template list. Press the **'Create Template'** button to store the template.
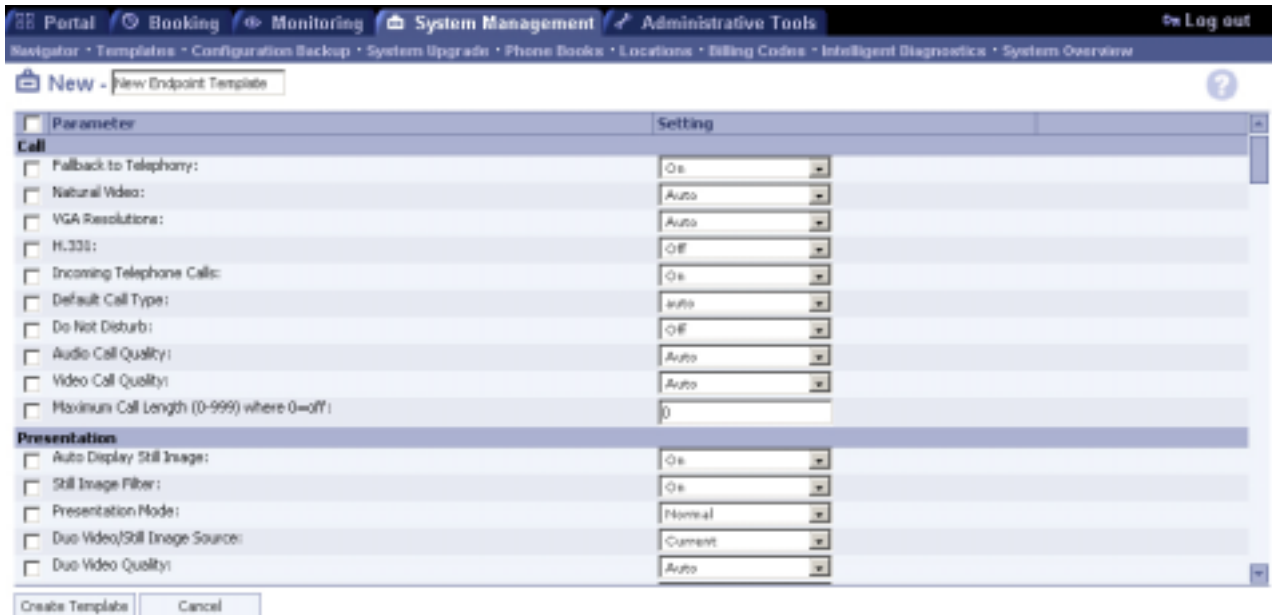
New Endpoint Template

New MCU Template

This template is used for TANDBERG MCU's. In the list of availlable settings, hook off and set the wanted value for all the settings you want to have in the new template list. Press the **'Create Template'** button to store the template.

Upload Logo

Upload Logos into TMS to be used as startup image on endpoints or miscellaneous images to set on the TANDBERG MCU. These images will be available in the Template settings.The systems only accepts images in JPG format.

Maximum Image sizes:

TANDBERG Endpoints with B5 Software and older:	320 X 200
TANDBERG Endpoints with B6/E1 and newer:	704 X 480
TANDBERG MCU:	352 X 288

Upload Sound

Upload sounds into TMS to be used as miscellaneous sounds to set on the TANDBERG MCU.These sounds will be available in the Template settings.
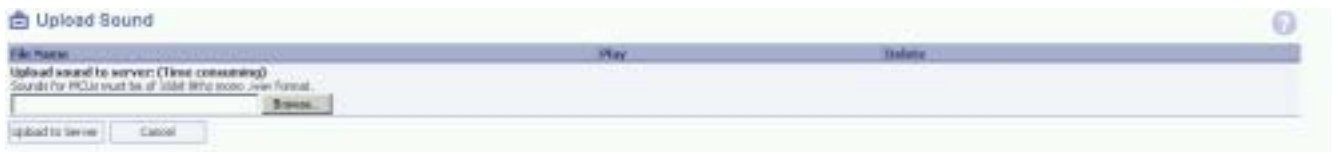
Viewing Templates

The templates can be viewed by clicking the '**View**' link. This will displays the settings that will be set on the selected endpoints or MCU's.

Editing Templates

The templates can be edited by clicking the '**Edit**' link.

All parameters in the templates can be changed. The settings are stored by clicking the **'Update Template'** button. Clicking the **'Cancel'** button takes the user back to the template list.
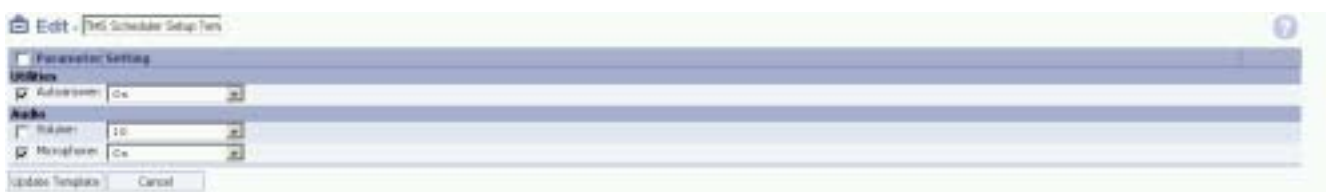
Tip: A template can be set up to handle as many settings as you like. If you only want to change the language on a set of systems. Select the language check box, and change the language.

Update Systems

By clicking the **'Update Systems'** link, a list of all systems registered in TMS will be displayed. Select the
systems you would like to update with the selected template. Press the **'Update selected'** button.

Configuration Backup
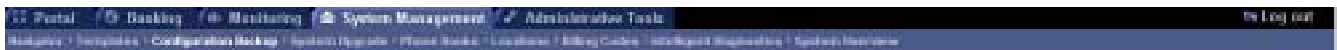
This feature allows the user to backup all the settings of several videoconferencing systems. Backup for later restoring of the systems settings is done in one operation.

System Configuration Restore in the configuration backup menu

In the menu on the left of the window there are two choices: Backup and Restore.

Backup

Here you choose which systems to backup on the TMS server. All the system configurations are stored on the TMS server for later restoring. Select systems, and press the **'Upload to TMS'** button. For systems that are already backed up on the server, 'Backup already exists' is shown next to the system name.

Restore

Only systems with a backup on the TMS server are available for selection in this menu. To restore the system settings, select the systems to restore to, and press the **'Download to Systems'** button. The settings stored on the TMS server as described above, are then restored to the system.

System Upgrade

To upgrade software on the videoconferencing systems from TMS, choose 'System Upgrade' in the menu.

Upload Software

In order for TMS to handle software upgrades of systems registred in TMS, the software versions first needs to be loaded into TMS.

Select '**Upload Software**' on the left-hand side menu to upload software versions to the TMS server. Click **'Browse'** to browse your computer for the software. Locate the appropriate file (*.pkg) to upload. After selecting a software package, click **'Upload Software'**. This may take some time. The file name is now shown in the list.
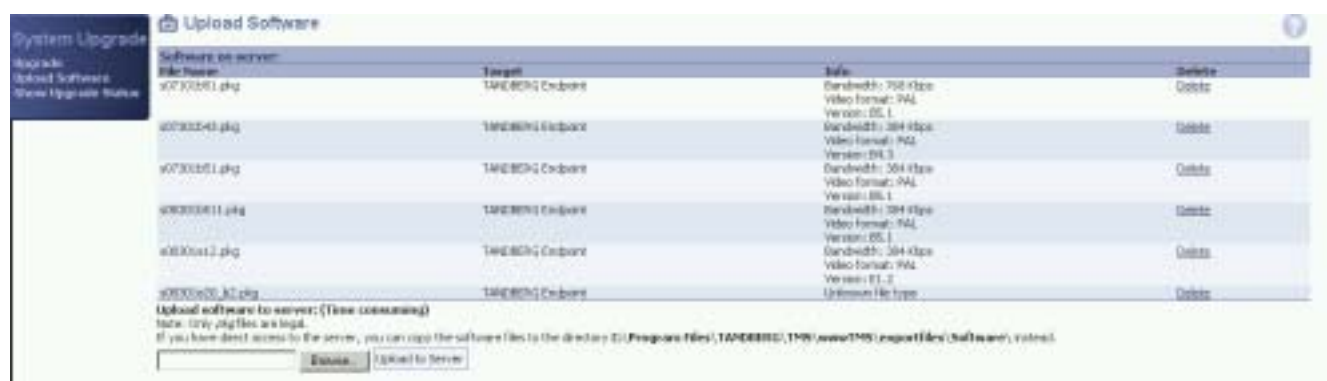
When a software package is no longer needed, it can be removed from the server by clicking the **'Delete'** link in the 'Upload software' menu.

If the user has access to the server he can copy the software packages directly into the destination directory of the server, instead of uploading them through the Administrator. The destination directory for the software is set under 'Administrative Tools' - 'TMS Configuration'.

Upgrade

In the 'Upgrade' menu, you select which systems you want to upgrade and what kind of upgrade mode you want to use.
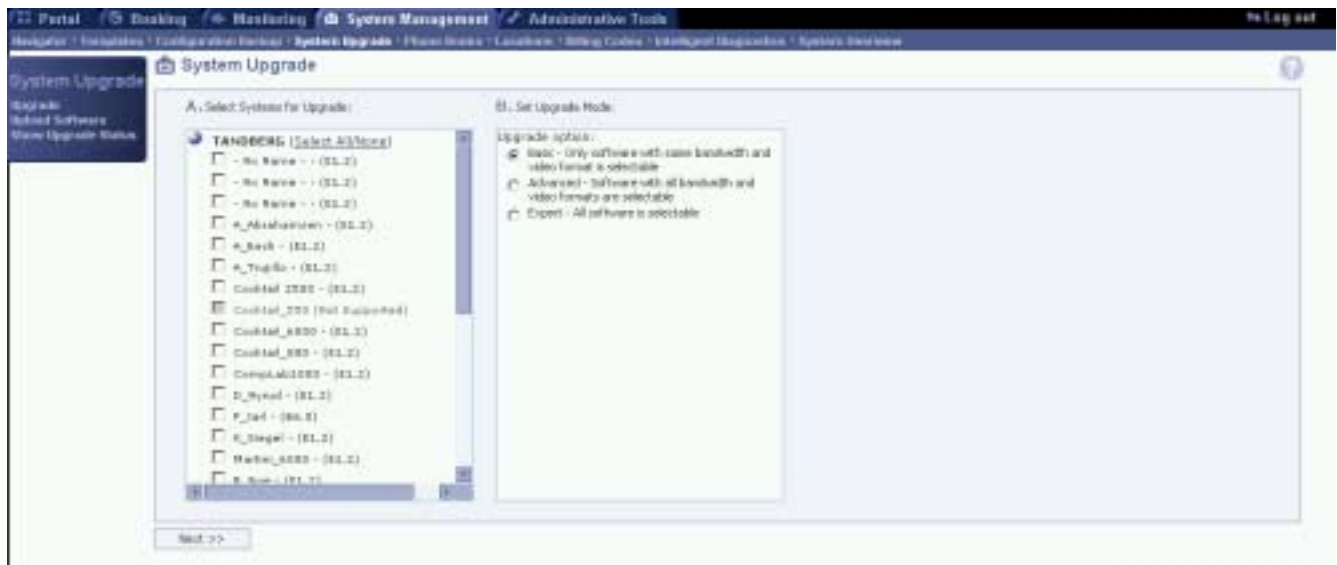
There are three upgrade modes available:

Basic Upgrade: TMS will select a software package that is compatible with the software already installed on the system. This is useful for upgrading to a newer software version.

Advanced Upgrade: TMS will select software packages with different bandwidths. Use the scroll bar to select software. This is useful for upgrading to newer software and/or upgrading to another bandwidth.

Expert: TMS will set up a list of all the software packages available on the TMS server

To upgrade the software versions of systems in TMS, you first need the new software loaded on the TMS server (see previous chapter). Secondly you need new Release Keys for the systems to upgrade.

To get the Release Keys you first need to generate a Release Key Report. Once you have made your selection of which systems you want to upgrade and which upgrade mode you want to use, press the '**Next**' button (see figure above: System Upgrade).

The next screen will show a list of each system you selected and show the compatible software available on the server. Select the systems you want to upgrade and the software file from the drop-down box to use for each system. You can now generate the release key report by clicking on the **'Generate Release Key Report'** button at the bottom of the menu. This will export a *.log file that contains information about the listed systems. The user can send this report to TANDBERG for release key generation.

Upon receival of the Release Keys from TANDBERG, you repeat the above procedure, i.e. select '**Upgrade**', select the systems you want to upgrade, and press the '**Next**' button. On the next screen, select the software version you want loaded on each of the systems from the drop-down box and then fill in the Release Keys received from TANDBERG.

Optionally you can select the '**Import Release Key Report**' and enter the log file received from TANDBERG using the 'Browse' button. Press the '**Import Report**' key when the log file has been located on your computer.

Select the '**Back**' button when the Release Key Log has been located and imported.
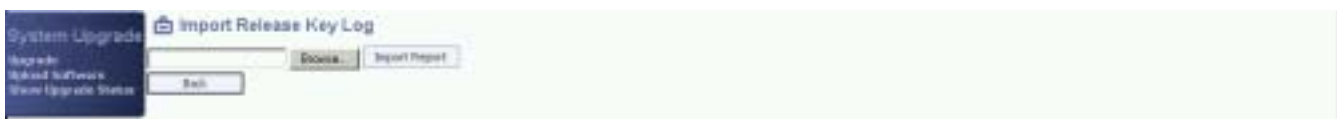
You can now choose to upgrade immediately by clicking on the '**Upgrade Now**' button or schedule the upgrade for later by clicking on the '**Schedule Upgrade**' button. Scheduled upgrades can be useful for upgrading systems during the night when it's unlikely that the systems are in use. Press '**Schedule Upgrades'**, and from the calendar choose the date, and also set the time for the upgrade. This option will upgrade two systems at a time, every five minutes.

Note: The time is related to the TMS-server time.

Show Upgrade Status

Status during the software upload process is shown in the 'Show Upgrade Status' located in the left menu. If a system is in a call the software upload procedure will not be carried out and the message 'Unit is in call, upgrading aborted' will be presented. If a software upload fails due to a wrong release key the message 'Wrong release key!' will be displayed.

Phone Books

TMS offers functionality for creating and administrating Phone Books, storing numbers for easy access. Different persons, organizations, departments, etc. may make their own TMS Phone Books.

TMS has powerful features for administrating Phone Books for systems. TMS Phone Books are managed by choosing **'Phone Books'** in the menu on the left side of the window.
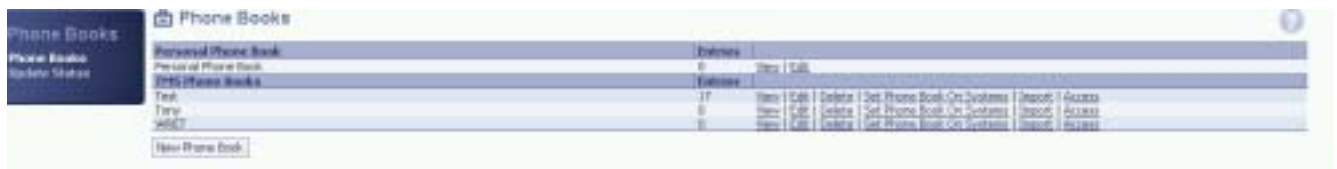
TMS Phone Books.

New Phone Book

To make a new Phone Book on the TMS server, click the **'New Phone Book'** button. Choose a name for the Phone Book and select the update frequency in the **'Update systems with this Phone Book'** scroll down menu and click **'Save'**. The new Phone Book is now shown in the list of all available Phone Books.

Edit Phone Book

Click **'Edit'** to the right of the Phone Book to be edited. Name, Number, Profile and Quality can be edited. The changes are saved with the **'Update Phonebook'** button. To delete one or more entries, click on the **'Delete'** check box beside the entries, and then on the **'Update'** button at the bottom of the page.

You can also set a update frequency for each phone book. The update frequency controls how often TMS will update the videoconference systems with a TMS Phone Book. These setting also controls how often TMS imports a Phone Book from an external device (LDAP, ILS, Gatekeeper).

Note: Only 5 new entries can be added at a time. To add more, select the 'Update Phonebook' button and then edit the phonebook again (with 5 new entries).

View Phone Book

To view a list of all entries in a phone book, click the 'View' link to the right of the phone book.

Below the list of entries, two buttons are available. They are named, **'Edit Phone Book'** and **'Phone Books'**. The **'Edit Phone Book'** button displays the edit phone book page already described in the previous chapter. The '**Phone Books'** button takes the user to the main 'Phone Book' page.

Set Phone Book On Systems

The **'Set Phone Book On Systems'** is used to select systems that will use this phone book as their global directory. Click on the **'Set Phone Book On Systems'** link which will give you the folder tree of systems within TMS. Select the systems to use the phone book using the checkboxes for each system, and press the **'OK'** button. TMS will start to update the systems with the directory in the background. Use the **'Update Status'** link in the left side of the window to check the progress.

Import

The Import function allows importing entries from a codec's directory, or from external resources such as ILS, Active Directory, Polycom GMS/LDAP, H.350 Directory and Radvision Gatekeepers. Clicking on the '**Import**' link for one specific phone book will take you to the following page, allowing you to import phone book entries from external sources.

An overview of already defined 'frequent import source' are listed on this page. These can be edited or deleted, by selecting corresponding link.

Importing phone book entries can either be done as a one-time event, or by scheduling regular imports.

One-Time Imports

One-time imports allows you to define in more detail which exact entries of an external source you want to import.
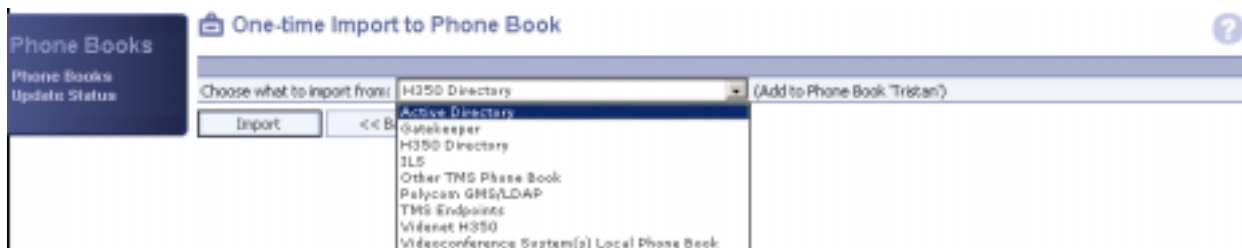
One-Time Imports

If you select to import entries from from a Specific video conferencing endpoint's local phone book, you will be presented with a scroll-bar where you can pich the videoconferencing endpoint to import from.

Select the desired system, and press the **'Import'** button at the bottom of the page. The local directory of the selected system will then be displayed. Select which entries to import by selecting their checkboxes, edit the entry you want to add to the phone book, and press the **'Import Selected Entries'** button. The Phone Book with the imported entries will then be shown.

Add Frequent Import Source

Selecting 'Add Frequent Import Source', imports all the entries of a given source. The phone book can also be scheduled to be updated from this source on a regular basis.

If you choose to import from a video conference system, select 'Import from a video conference system' and press **'Import'** You will be shown the folder tree of the systems in TMS. Select the desired system, and press the **'Import'** button at the bottom of the page. The local directory of the selected system will then be displayed. Select which entries to import by selecting their checkboxes, edit the entry you want to add to the phone book, and press the **'Import Selected Entries'** button. The Phone Book with the imported entries will then be shown.

Note: Only TANDBERG systems with software versions B3 or higher can be updated with a TMS Phone Book.

Export

To export phone book entries from TMS to an external system, select '**Update Type**' to be '**Update TMS and External**'.

Locations
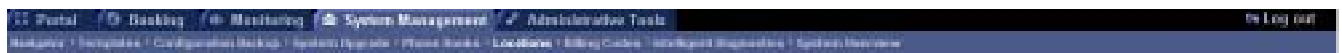
'Locations' defines the physical locations where your different videoconferencing equipment is placed. Different parameters can be assigned to each 'location', including time zones, access codes, prefix'es used, etc.It is important that every videoconferencing equipment managed by TMS is allocated to a location. In particular this is importent for TMS to manage scheduling of calls.
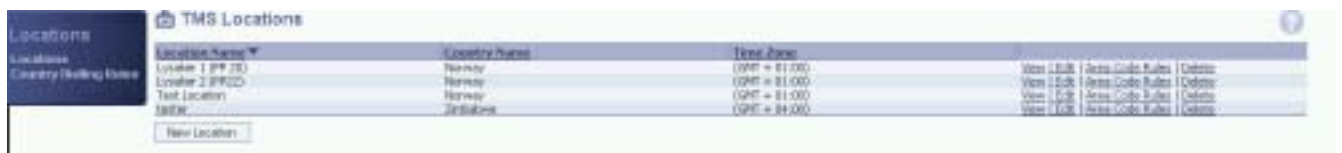
By pressing '**Edit**' at the right in the menu, all locations and routing settings may be changed. These settings are described in the chapter 'New Location'. If '**Delete**' is pressed, the location will be deleted from the TMS server.

New Location

Press '**New Location**' to define a new location in TMS.

Create a new location.

Location Name

Name of the location. Try to be descriptive of the location your specifying.

Country/Region

The country for the location. This gives the system information about the country code and dialling rules for that country.

Time Zone

The time zone for the location.

Area Code

The locations area code (This field can be left empty if an area code is not used in the country selected).

To access an outside line for local calls

Number to call for accessing an outside line for local calls (calls between systems in the same area code).

To access an outside line for long distance calls:

Number to call for accessing an outside line for long distance calls (calls between systems in different area codes or countries).

Gateway Prefix

The prefix to call when making calls through a gateway. TMS will allow systems without ISDN-lines to make ISDN calls if the location is set up with a gateway prefix, set up to use a gateway and the system is registered to a H323 gatekeeper. It is recommended to set the gateway prefix to be the auto bandwidth prefix of the gateway being used. Please refer to the gateway documentation to set up the systems correctly.

Gateway uses ISDN prefixes

Check this box if the gateway must use the same rules for accessing an outside line as specified above in 'To access an outside line for local/long distance calls'.

ISDN default for systems in same location

TMS gives you the option to prefer ISDN or IP calls to be made between systems in the same location.

Number of digits to use for internal ISDN calls

Specify the number of digits required to connect to another system within the same location.

Prefer IP/ISDN when dialling from this Location to the following other locations

When dialling between locations, TMS by default uses ISDN as the preferred mechanism for setting up the call. This field allows you to change the preferred dialling mechanism between this Location and the other locations defined in TMS. It is only recommended to use IP as the preferred mechanism if there is a dedicated IP connection between the two locations in question.

Press **'Save'** to store the settings for the location.

Area Code Rules

Area code rules are typically used in the US to set up 10-digit dialling and area code overlays. Area code rules determine how ISDN-numbers are dialled from one area code (the area code set for the location) to other area codes.

To add or edit an area code rule for a location, click '**Area Code Rules**' on the right side of the desired location. After clicking the link, a page with an overview of all area code rules for the location is displayed.

Overview of area code rules for the location 'New York'. From this page, new rules can be added to the location by pressing the button 'New Rule'. Old rules for the location can be edited or deleted by pressing the links **'Edit'** or **'Delete'** on the right of every rule.

Note: US phone number, e.g. +1 (123) 456-7890, the area code consists of the digits in brackets (123), and the prefix consists of the following three digits, in this example,the digits 456.

Create a new dialling code for the selected location by selecting the '**New Rule**' button'.

When adding a new rule for a location, fill in the fields as described below:

Field 1. 'When dialling from 'area code for location' to the following area code'

This field, combined with the prefix field explained below, decides the area code that this rule applies to. It may be set to be the same area code used for the location.

Field 2. 'With the following prefixes'

The rule will only apply to the calls made to the area code in Field 1, with the prefixes listed in Field 2. If this field is left empty, the rule will apply for all calls made to the area code in Field 1.

Checkbox. 'Include the area code being dialled'

If checked, the area code in Field 1 will be included in the call. If unchecked, the area code will not be included in the call. For the US, check this checkbox to enable 10-digit dialling.

Field 3. 'Before dialling, also dial'

If the rule applies, as stated in Field 1 and Field 2, the digit(s) in this field will be dialled first when making a call. In most cases this field will be empty.

Select '**Save**' when you are done defining your new area code for this loation.

Note: When an Area Code rule is used, prefixes from the location profile are still used, but domestic dialing behaviors (such as inserting a 1) are ignored by TMS.

Billing Codes

Billing code is a protection mechanism, allowing you to control the usage of certain videoconferencing systems.If Billing Code protection is set on a system, it is not possible to make a call from it without entering a valid billing code. Billing codes are much like password protection on a videoconference system. Notice that there is no problem to call into a system protected by billing codes.

Billing Codes are stored in TMS with a description. The description is there to make it easier to identify what the billing codes are actually used for.

The TMS has powerful features for controlling the Billing Codes functionality on TANDBERG videoconference systems. To edit any billing code, enter the '**System Management**' and '**Billing Codes**' menu on the top of the window. In TMS the billing codes can be uploaded to all systems supporting these codes.

In the left menu the user has two options. Edit Billing Codes and Update Systems.

Edit Billing Codes
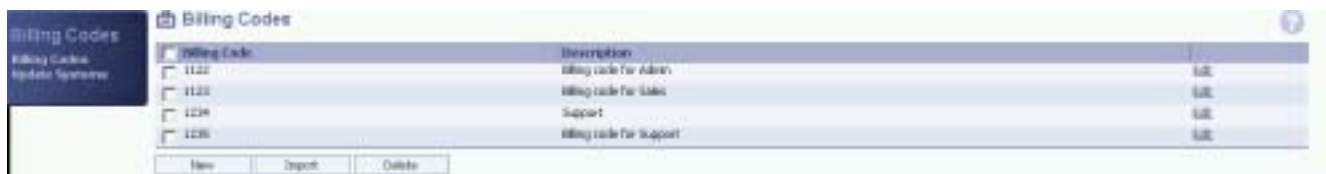
List of billing codes.

To make a new Billing Code, click the '**New**' button. Type the billing code and its description in the text fields, and press '**Save**'. The new billing code will then be shown in the list of billing codes.

An billing code can be edited by clicking the '**Edit**' button to the right of it. To delete an billing code, check the checkbox to the right of the billing code, and press the '**Delete**' button. The deletion needs to be confirmed by pressing the '**Confirm**' button.

Import Billing Codes

Billing codes can be imported into TMS by selecting the '**Import**' button. You will then be allowed to copy a set of billing codes into a text field. Importing billing codes requires the text feld to be populated with one billing code followed by a description on each line. Select the 'Import' button at the bottom of the screen to import the billing codes.

Import billing codes

Update Systems

It is also possible to force the use of billing codes directly on specific endpoints. This means that calls can not be initiated from the remote control of these system without entering a billing code first. Billing codes on systems can be set to '**Required**', '**Optional**' or '**Not in use**'.

To activate billing codes on specific videoconferencing endpoints, select '**Update Systems**' in the right-hand menu.

Select systems to update with billing codes.

Check off the systems for Billing code activation (or deactivation) in the left window, and choose between three billing codes options in the right window:

• *Require billing code before making calls.*
  A valid code must be entered before the user can make a call. This code will prevent unauthorised users making calls and for authorised users it can be used for billing. A system can have several billing codes.

- *Ask for billing code before making calls.*
  This code will not prevent unauthorized users from making calls. The code that is entered before making the call will be assigned to a user or a group for billing and/or statistics.

- *Turn off billing code use.*
  The system will not ask for any code before the user can make a call.

Select 'Update Systems' when finished. A message 'Starting system update' will appear on the screen, and a confirmation will be given when the systems are updated.

Note: Setting billing codes on a system does not affect calls being initiated from TMS (i.e. where TMS informs the endpoint to initiate a call). TMS can however be set up to require billing codes to be entered also when booking conferences using TMS. See Advanced Use - Administrative Settings for more details.

Intelligent Diagnostics

In this page you will see a list of all systems registered in TMS with a diagnostic message for each system. Error messages are in red text and warnings messages will be shown as yellow text. By clicking on a field name on the top of the list, the list will be sorted alphabetically based on the values for that specific field.

Also note the check-boxes in the upper right hand corner, allowing you to narrow down the list according to your preference.

List of diagnsostics for all systems in TMS.

For more detailed diagnostics on a particular system, click on the system name in question. A separate diagnostics page for that system will then be displayed.

For settings that are not correct, TMS will suggest a valid setting for those settings. In the next picture, three errors are detected: Location, TrapHost IP address and SNMP Community Name. By replacing the current settings with the suggested settings found in the red text and then pressing the **'update'** button, this system will work in conjunction with TMS and will be shown as 'OK' in the 'Intelligent Diagnostic' page.

System Overview

The System Overview function allows you to view specific parameters on specific systems, and have these presented in nice and well arranged way.

System Overview

On the left hand side, you select the systems you want to get an overview of, while you on the right-hand side ticks off the parameters you want listed for each of these systems.

The parameters 'System Name' and 'IP address' are by default always checked.

For instance, if you want to check the SNMP community name of all your systems, click the 'Select All/None' link for selecting all systems on the left-hand side, and then tick off the SNMP Community Name parameter option on the right hand side.

Select '**View**' to view a printable list of the SNMP community names of all your systems.

Advanced use

Administrative Tools

TMS Configuration

Click on the '**TMS Configuration**' link under '**Administrative Tools**' in the top frame of the window to get access to the configuration page of the TANDBERG Management Suite.

TMS configuration page

All the parameter settings in TMS are grouped into the following cathegories:

> TMS Settings
> System Interface
> Trap Agent Configuration
> SMTP/Mail Settings
> Booking/Scheduling
> Web Conferencing

Each of these cathegories are grouped into corresponding folders under TMS Configuration, and all the parameters listed in these folders will be described in the following chapters.

TMS Settings

TMS License Key

TMS License Key is a key, which configures how many systems you are allowed to add in your TMS installation. The default key only allows for up to three systems to be added. If you have received a TMS license key from TANDBERG or distributors, please enter this key here. Entering an invalid key will default TMS to run as a three-systems version.

TMS Default Location

The default location to use when adding new systems to TMS. See 'System Management' - 'Location' for more information.

TMS Default Time Zone

Select the default time zone for new users added to TMS.

Statistics history

The default number of days to use for showing system statistics. E.g. If this value is set to 5, viewing the call activity statistics log for a system will by default show call activity statistics for the previous 5 days.

Note: Pressing the link 'Set Location on Systems' will lauch a window allowing you to easily assign locations to systems. An overview of all the systems registred in TMS will be listed, with the possibility to change the location information (select location from scrollbar).

Scripting Timeout

Scripting Timeout (in seconds) describes how long a script may run on the server before it times out.

Software FTP Directory

Software FTP Directory is the directory on the server where the system software is stored to be used for system upgrades. This directory must already exist, it will not be created by updating this page. In addition, this directory must have 'write' abilities for everyone (i.e. admin, user etc). The software stored in this directory can then be used to upgrade systems.

System Navigator Cache Mode

The System Navigator Cache Mode setting determines when TMS will connect to the system when the user clicks on the System Information page of the system in System Navigator. The default is that it refreshes when cached data is old. To have TMS behave like older versions of TMS (before version 7), set this setting to 'Always Refresh System Information'

Note that this setting Only applies to the 'System Information' tab - the other tabs, like 'Other System Settings' and 'Phone Book' etc. will always retrieve the information directly from the system.

System Settings Cache Timeout

System Settings Cache Timeout is how old the cached system information data can be before it requires refreshing. The setting is used by the TMS Watchdog Scanner which will use the setting to determine whether the cached systems data needs refreshing or not. If the setting 'System Navigator Cache Mode' is set to refresh if cache is old, this setting will also affect the System Navigator. Note that the cached information is also used by TMS to determine available resources when scheduling calls. It is therefore important that the refresh timeout is not set too high. The default is One Day. Note that setting the timeout too low may cause a lot of unneccessary traffic on the network.

Show Local View Snapshots in System Information Page

Depending on the system type this will show a snapshot taken from the camera of the system. This is independent of the system being in call or not. Note that the snapshot will only appear if the client computer (not just the TMS server) has direct LAN connection to the system. If not the image will appear as a missing object in the browser (Red X in MS Internet Explorer). This function is therefore not recommended for remote administration of systems through e.g. a firewall.

System Interface

Telnet Timeout

Telnet Timeout (in seconds) is for how long the server will wait for a response when trying to initiate a Telnet session.This timeout must not be set too high because if some systems are not reachable, the page might take several minutes to load (usually 3 seconds are fine).

FTP Timeout

FTP Timeout (in seconds) is how long the server will wait for a response when trying to initiate a FTP connection (i.e. software upload, system setting backup).

Message Timeout

Message Timeout (in seconds) is the default amount of time a message is displayed on a system when using the 'Send Message to Codec' feature.

SNMP Timeout

SNMP Timeout (in seconds) is the time TMS will wait for a reply from an SNMP query. One second should be ok, but if you find the feedback is incorrect from the system, it may need to be increased.

SNMP Community Name

SNMP Community Name is by default set to public. This SNMP Community Name is a password that the TANDBERG Watchdog use when requesting SNMP variables from the system. Enter a comma separated list of all the community names used on the systems in your network.

Set SNMP Community Name on Systems

Set SNMP Community Name gives functionality to update the SNMP Community Name on all systems added to folders in TMS.

If the SNMP Community Name on a system is different from the one entered in the first 'SNMP CommunityName'-field in the configuration page, you can update it by checking the checkbox to the right of the codec name and click on the **'Update'** button.

Systems that already have the correct SNMP Community Name will be listed as a verification of this. These are grayed out, and can not be updated.

Systems that do not respond will not have the checkbox making it possible to set the SNMP Community Name, but are listed with a message saying that they did not respond.

SNMP Trap Host

SNMP Trap Host is the address of the SNMP server waiting for the traps and is usually the TMS server IP address. Click on the link to the right to set this address on one or several systems.

Set SNMP Trap Host on Systems

Set SNMP Trap Host gives functionality to update the SNMP Trap Host Address on all systems added to TMS. If the SNMP Trap Host on a system is different from the one entered in 'SNMP Trap Host'-field in the configuration page, you can update it by checking the checkbox to the right of the codec name and click on the 'Update' button.

Systems that already have the correct SNMP Trap Host Address will be listed as a verification on this. These are grayed out, and cannot be updated.

Systems that do not respond will not have the checkbox making it possible to set the trap host address, but are listed with a message saying that they did not respond.
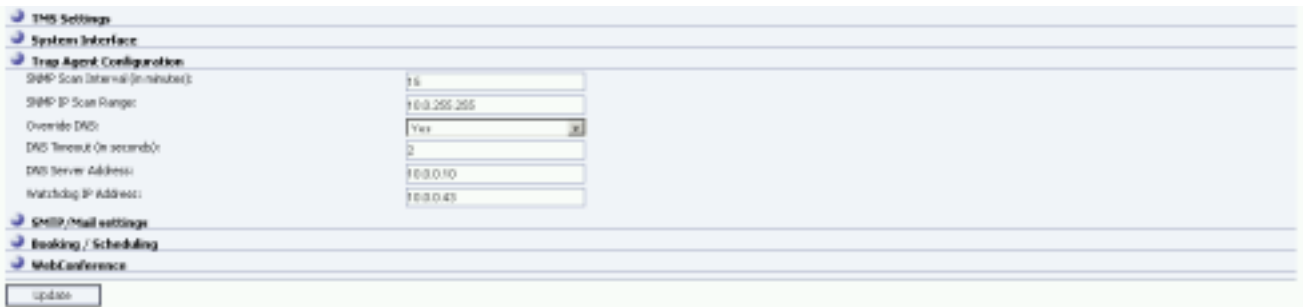
Boot Wait

Boot Wait (in seconds) is used during software upgrading of a system and is the time the server will wait when the system is rebooting before trying to perform actions on the system (i.e. restoring of settings). In most cases 45 seconds will be sufficient.

Boot Retry

Boot Retry is used in conjunction with 'Boot wait' and will only be used if a system has not rebooted within the time entered under 'Boot wait'. The 'Boot retry' is the number of times TMS will go back and start the 'Boot wait' timer again. In most cases 5 times will be sufficient.

Trap Agent Configuration

SNMP Scan Interval

SNMP Scan Interval is how often (in minutes) the TANDBERG Watchdog scans the network to see if all the systems are still reachable, and to discover new systems in the network. If a system is no longer reachable, its status will be set to 'No response' and will stay in this condition until it is reconnected again and detected by a network scan or it makes a video call.

SNMP IP Scan Range

SNMP IP Scan Range is the subnet TANDBERG Watchdog is scanning. By default TANDBERG Watchdog scans the entire network for systems i.e. sends a broadcast to the address '255.255.255.255'. This address is possible to change and also be configured to work with your network. A possible value can be '10.0.255.255' where TANDBERG Watchdog will get response from systems connected to the '10.0' subnet. To only monitor a specific system, type the IP- address of the system. Multiple scan ranges may be entered by seperating the entries with a comma.

Override DNS

Set this to 'Yes' if you want to use the IP address of systems instead of trying the DNS-name when identifying systems.

DNS Timeout

DNS Timeout (in seconds) is how long a DNS query will wait until the request times out.

DNS Server Address

Set this value to the IP-address of your DNS server.

Watchdog IP Address

Contains the IP address where the TMS Watchdog is running. By default it is set to the IP-address of the TMS server.

SMTP/Mail Settings

From Mail Address

The 'From Mail Address' is the email address TMS poses itself as when sending email notifications. The address will show up in the 'From:' line of the reciever's email client.

SMTP Server

Set this value to the IP-Address of your SMTP (Mail) server.

SMTP Server authentication Username

Put in the username to access the mail server if this is required

SMTP Server authentication Password

Put in the password to access the mail server if this is required

Booking/Scheduling

Connection Attempts for Scheduled Calls

Connection Attempts for Scheduled calls is the number of times TMS will attempt to connect calls if a call is not successful.

Connection Timeout for Scheduled Calls

Connection Timeout for Scheduled Calls is the number of seconds to wait for a successful connection. If a system does not connect within this time, the call will be disconnected and retried the number of times set in the 'Connection Attempts for Scheduled Calls'.

Default Conference Title

The default title used for all booked/Scheduled meetings. This can be edited in the Booking/Scheduling wizard.By default this is set to 'Untitled'.

Default Scheduled Call Duration

This is the default conference duration used for bookings and schedules.

Default Bandwidth

Allows you to specify the bandwidth that will be used by default in the Booking/Scheduling wizard .

Default Picture Mode

Specifies the default conference picture mode. You can choose between voice switched and continious presence

Billing Code for Scheduled Calls

Billing Code for Scheduled Calls indicates whether or not billing codes are required for scheduling calls using TMS or Scheduler. Options here are 'No', 'Optional' or 'Required'. If set to 'Required', users will not be able to schedule a call without entering a valid billing code. See Billing Codes under System Management.

Default Extension Option

Default Extension Option specifies whether the option to extend a meeting from the remote control by default should be checked off when making the reservation.

Hide name of conference owner for other users

Indicates whether or not the conference owners name should be visible for other users.

Contact Information to extend meetings

TMS displays an 'To Extend Meeting' message on compatible systems 1 and 5 minutes prior to the end time of a conference. This field allows you to customize what follows the Extend Meeting message. Enter contact information like telephone number or name of contact person.

Allow changing advanced settings in TANDBERG Scheduler

Specify who should be allowed to access the 'Advanced Settings' in the TANDBERG Scheduler. The options are: none, administrator only or all.

Default language for use in TANDBERG Scheduler

Defines the default language used for new users of TANDBERG Scheduler. For new users, all texts in TANDBERG Scheduler will be in this language. Users can choose between 13 different languages from the user preferences page.

Company Logo

You can install your own company Logo. This logo is used in the TANDBERG Scheduler.
The file must be in .gif format.

Scheduled Calls must be approved before they can connect

When this setting is set to yes, all videoconferences booked by none-administrator users, needs to be approved before they can connect. Conferences can be approved from the Conference Control Center page and the All Meetings page in TMS.

Default reservation type for scheduled calls

Indicates what the default reservation type for scheduled calls should be set to. Options here are 'Automatic Call Launch' or ' Reservation only'.

Web Conferencing (Optional)

Web conferencing is an option provided by TMS, allowing web based conferencing to be scheduled together with a video/audio conference. Different web conferencing solutions are available, dependent upon the end users' needs. Please note that web conferencing requires a separate service agreement or server installation (dependent upon solution chosen). See chapter on '*Web Conferencing*' for further information.

Enable Web Conference support

If selecting TANDBERG See&Share, the following parameters will have to be specified (see snapshot above):

Web Conference Server DNS name

Enter host name of the See&Share server you want TMS to connect to.URL address of the Web Conference server that will be used.

Remote control password for See&Share server

Enter the password for being allowed to create web conferences on the See&Share server. This password is defined on the See&Share server (using Admin application).

Enable Web Conference support

If selecting WebEx, the following parameters will have to be specified:

Web Conference Server URL

Enter URL address of the Web Conference server that will be used.

Please use the following format: *http://URL*

Password for WebEx server

Enter the password for the WebEx conferencing server.

UserName for web conferencing server

Enter the User Name for the web conferencing server, provided by the web conferencing service partner.

SiteID for web conferencing server

Enter the SiteID for the web conferencing server, provided by the web conferencing service partner.

PartnerID for web conferencing server

Enter the PartnerID for the web conferencing server, provided by the web conferencing service partner.

Note: The WebConference connection status indicates whether or not TMS has been able to connect to the defined server. This parameter will automatically be updated after you have given you input to the paramters above and selected the 'Update' button.

User Administration

User Administration controls which users have access to which parts of TMS. Access rights are controlled on a group level (i.e. you assign rights to a group). The total access level for an end user will then be the sum of all the rights assigns to all the groups that the end user is a member of. Note that an end user can be (and in most cases are) a member of several groups.

There are 3 pre-defined groups in TMS. These are the **Site Administrator**, the **Video Unit Administrator** and the **Users** groups.

The **Site Administrator** group has full access to all functions, folders and systems in TMS. Only people who could be put responsible for TMS functioning properly should be members of this group. Only the Site Administrator has access to the Administration Tools folder in TMS, i.e. only Site Administrators can add user, define groups, edit the TMS Configuration page.

The **Video Unit Administrator** (**VUA**) group has full administrative rights to ALL video conferencing systems (including gateways, gatekeepers and MCU) in your network. Typically the technical engineers are members of this group. Video Unit Administrators do not have access to the TMS Configuration page - otherwise, they have the same rights as the Site Administrator.

The **Users** group is a group that ALL end users automatically become a member of. It is recommended that the access rights assigned to this group represents the lowest level you want any person in your organisation to have. This applies to both what TMS functions you want them to see, as well as which systems they are allowed to use (see **Setting access rights on a system** for further details).

Click on the **'User Administration'** link under **'Administrative Tools'** in the top frame of the window to get access to the User Administration page. The group definitions will be presented:

From this page you can create new groups, or edit existing groups by clicking on the '**View/Edit**' link for a group. These features will be described in the following chapters.

*Note that you are not allowed to change any of the permission rights for the Site Administrator and Video Unit Administrator groups. Also, you can not add or remove users belonging to the **Users** group as all users by default is a member of this group.*
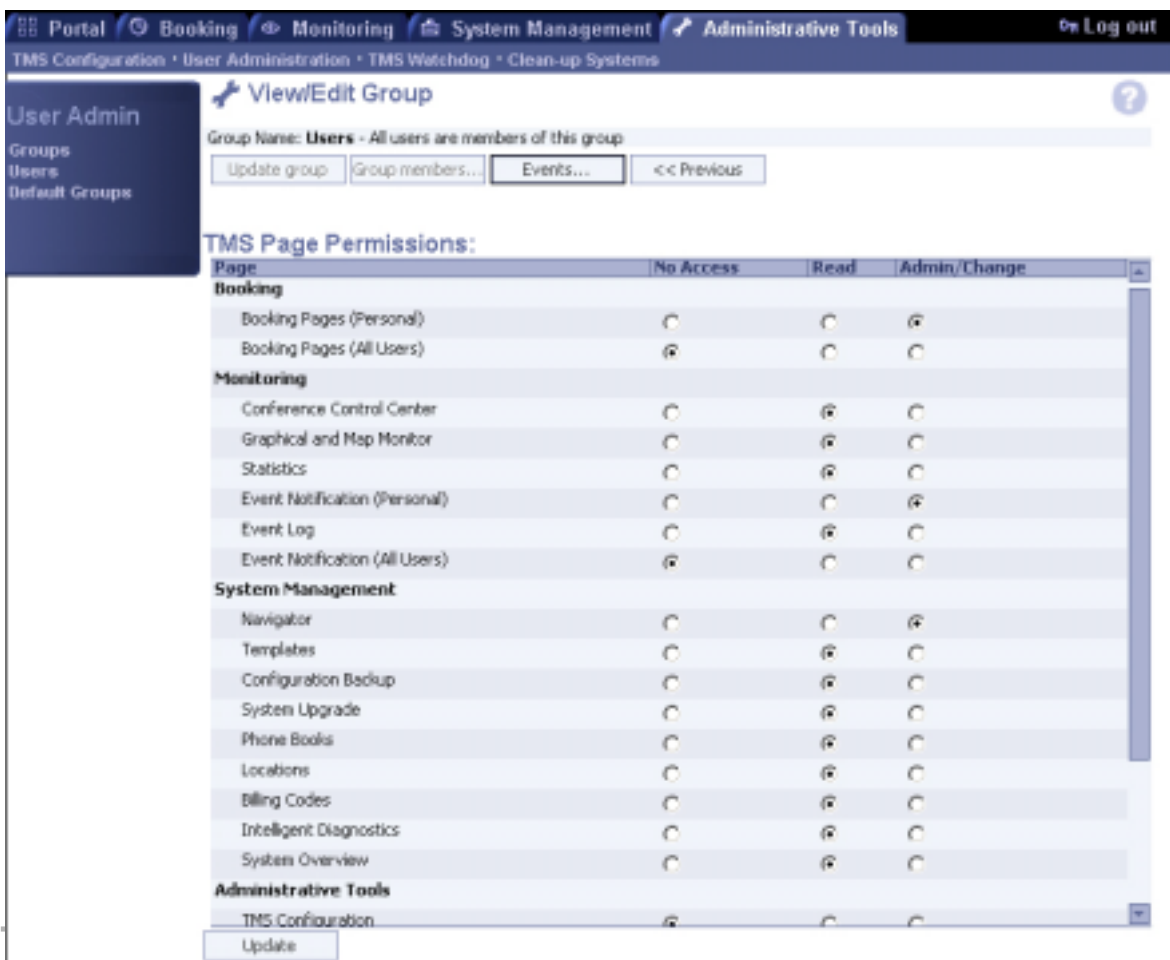
New Group

You can create new groups by clicking on the '**New Group**' button below all the listed groups.

Fill in the name of the group and a description for this new group and click on the '**Add group**' button. The group will then be created, and you are automatically presented with the View/Edit page of that group.

You can now add (and remove) members to the group, select which events members are allowed to subscribe to and define the TMS functions (web-pages) that will be available for the group memebers.

Group Access Rights

The Group Access Rights defines which which components of TMS the group members have access to. The three access levels to these components are

• **No Access** - The group members have no access to the given component of TMS.

• **Read** - The group members can view the contents of the given component of TMS, and use functions provided by the component on video conference systems the user also has Monitor or Admin rights to (see **Setting Access rights on a system**, later in this chapter).

• **Admin** - The group members can view and modify the content of the given TMS component.

When defining new groups, it is important to keep in mind that all users automatically also are members of the Users group. Any access rights given to the Users group will then apply to all users. Please make sure that the access rights defined for the Users group is the 'lowest' level you would like any user in your organisation to have. The default setting of the Users group access level can be used, but it is also possible to further restrict (or increase) these settings.

Having set the access rights to the Users group to the appropriate level, it is recommended that new groups that are created only defines the additional rights that members of this group should have (i.e. those rights that differs from the rights of the Users group).

Group Members

To add members to the group, click on the '**Group members**' button.

A list of the existing group members are presented to the left. To remove any of these members from the group, check off those users and click on the '**Remove selected users**' button.

To add new members to the group, select the new user from the scroll-down menu on the right hand side and click on the '**Add user**' button. When done editing the group-membes, select the '**<< Previous**' button to return to the main View/Edit page for the group (see picture on previous page).

Events

You can define which events that are available for subscription for each group.This means that group members will have the possibility to subscribe to these event. Defining the events for a group is done by clicking on the '**Events**' button for that group. Note that the actual subscription of the events for the individual group members are done under '**Monitoring**' - '**Event notification**'.
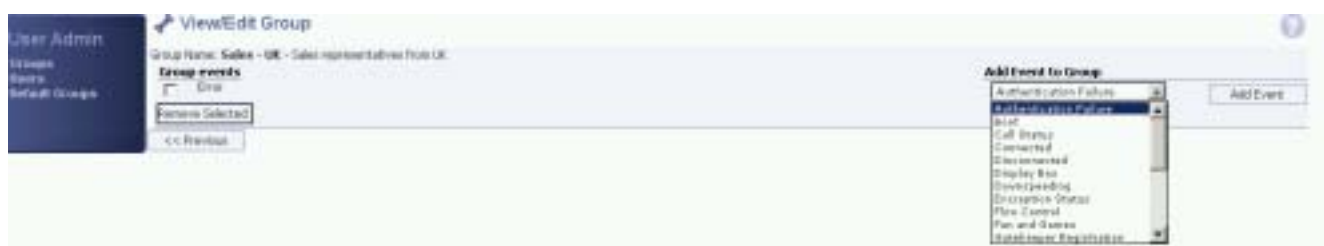
A list of the existing events are presented to the left. To remove any of these events from the group, check them off and click on the '**Remove selected**' button.

To add new events to the group, select the event from the scroll-down menu on the right hand side and click on the '**Add Event**' button. When done editing the event page, select the '**<< Previous**' button to return to the main View/Edit page for the group (see picture on previous page).

Note: Users can be members of several groups.A users access level equals the sum of all the rights defined in all the groups thatuser is a member of.

Users

To add a new user to TMS or edit an existing user account, press the **'Users'** link on the menu on the left hand side.

A list of all the registred users are listed. From here, new users can be created and existing users can be edited or deleted. Selecting '**New User**' or '**Edit/View**' on an existing user will cause a profile window for that user to appear - alternatively an empty profile for a new user.

Here you can change/insert any of the parameters related to that user. The parameters here are more or less self-explanatory, but please note that the user's NT-login name is important as this is used for authentication of the user.

When done editing, click on the '**Update User**' button to store the user's data.

Note: you can not delete your own user representation nor edit your own NT-login parameters while logged on.

User Login

A user is automatically added as a new user to TMS the first time the user accesses TMS. TMS will automatically detect the NT login Name of the user. TMS will also try and detect the users first and last name; this is not always possible. Therefore the user will be prompted to fill out this information the first time. A pop-up window will appear asking the user to fill in the users personal information. The user must also provide an email address. All fields must be filled in and the email address must be on the form xxx@yyy.zz. This pop-up will not disappear until all fields are filled in with valid information. Failing to do so will result in the window re-appearing.

Note: Users must be members of the Windows Network to be able to be users of TMS.

Default Groups

Default groups define which groups a new user automatically will be assigned to when registrating into TMS for the first time. Click on the '**Default Groups**' link on the menu on the left hand side.

By default all users will be member of the 'Users' group (can not be changed). In addition, the TMS administrator may here set which other groups new users automatically shall be members of.

To change the default group settings, check off the wanted groups and click on the '**Update Default**' button.

Authentication of users

Depending on the settings on the web-server, the users may be automatically logged on to TMS if the user is logged on to the same domain network as the TMS server (using NTLM – challenge response), or the users may be required to enter their NT login name and password. If a user is not logged on to the same domain as the TMS server, the user will be prompted to enter their NT login name and password.

If you want to allow for automatic authentication of users logged on to the same domain as the TMS server, do the following on your TMS server:

Press '**Start**' and go to '**Control Panel**' under '**Settings**'. Open '**Internet Services Manager**' under '**Administrative Tools**' – Right click on the virtual directory '**Default Web site - TMS**' – select '**Properties**'.
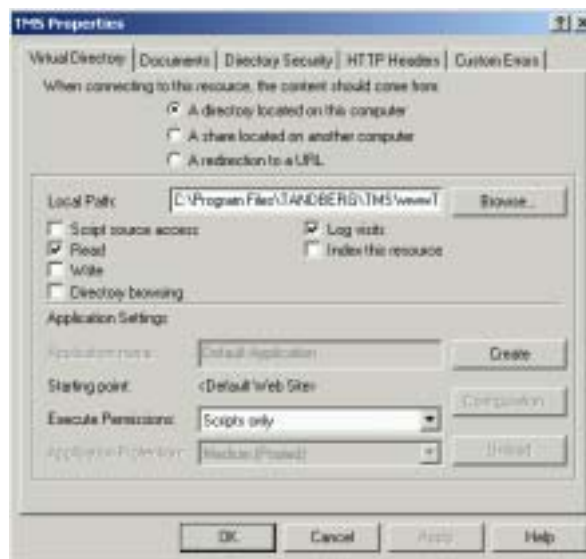
Virtual directory settings in Windows.

Select tab **'Directory Security'** – press **'Edit…'** button. Check off **'Integrated Windows Authentication'**.
Leave **'Basic Authentication'** checked to allow for login from other areas of the network.
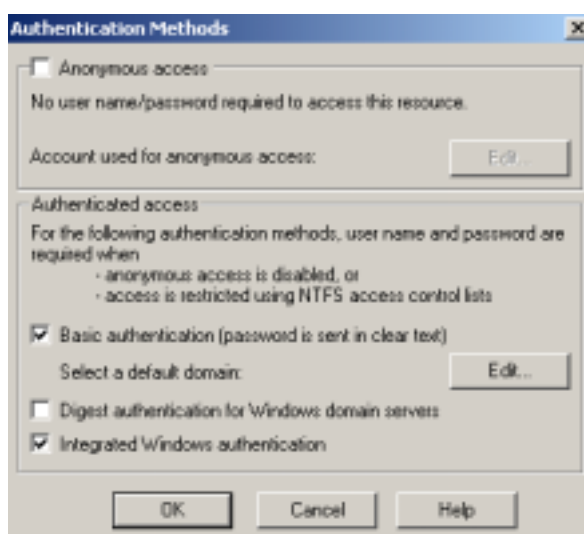
Authentication methods in Windows

To save the users from having to type in the user username in the form '\domain\username', press the **'Edit…'**
button next to the **'Basic Authentication'** checkbox and fill out the default domain name with the name of the
domain where the users are defined. The users can then simply use their 'username' instead of having to enter
the domain name each time they log on to TMS.

Access rights to systems and folders

TMS offers the possiblity to set access rights to both systems and folders. There are defined 4 different access levels to folders and systems. These are: No Access,Book,Monitor, and Admin

Setting access rights on a folder

Under '**System Management - Navigator** 'all systems registred in TMS are organised in folders. Access rights to the folder can be set by clicking the '**Folder Access**' button when viewing the content of the folder in question.

This page allows you to set the access right to this folders for all the defined groups registred in TMS. You can also tick off '**Apply to all subfolder**' to have the settings work recursively on all sub-folders. The settings can also be applied directly to each system in this folder by checking off the '**Apply to systems in folder**'.

The different access levels gives the following rights:

No Access: The users have no access to this folder. The folder will not appear in the 'System 'Navigator' for users without access.

Book/Monitor: The users have access to systems found in this folder.

Admin: The users have access to systems found in this folder. The users also have permission to add/ remove subfolders, rename folder, add systems to folder and set permission to folder.

Note: For a user to have access to a system, the user needs to have access both to the folder where the system is found and to the system itself. Also note that a system has only one set of access rights stored, even if the system is represented in multiple folders. The last stored settings of a system is the one that is valid.

Setting access rights on a system

Under '**System Management- Navigator**' you can set access rights on a system by clicking on the '**System Access**' link for that system.
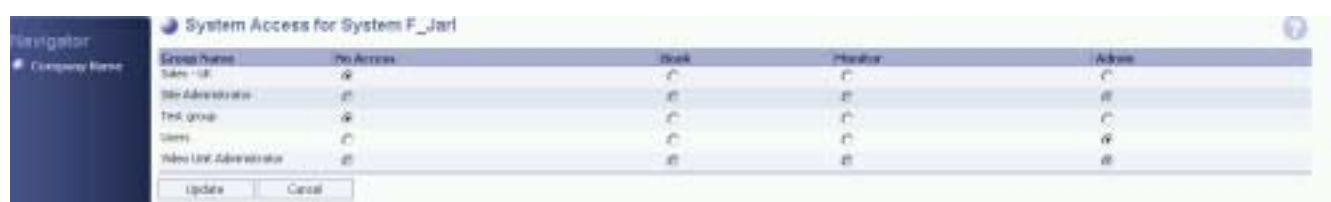
This page allows you to set the access right towards this sytem for all the groups defined in TMS. The different access levels gives the following rights:

No Access: The users have no access to this system. The system will not appear in the System Navigator for users without access.

Book: The users have access to use the system for dialling and scheduling.

Monitor: The users have access to the system for dialling, scheduling and viewing of settings and status. The user is also allowed to monitor its use using the graphical call monitor, event handler application and statistics.

Admin: The users have full access to the system, including software upgrade systems settings backup/restore, directories and changing system settings.

Note: *Site administrator group rights cannot be modified for systems. Read the Appendix for detailed information regarding different access rights.*

TMS Routing

TMS Routing ensures that videoconference calls are set up according to lowest cost and best video quality. TMS Routing is used in the TANDBERG Scheduler and in the TMS Booking. TMS Routing considers location, area code rules and available bandwidth for systems when setting up calls. It can route both ISDN and IP calls.

An easy example illustrates the power of TMS Routing. If setting up a call between two video conference units in the US and one in England, where all three units have internal MCUs, then the TMS Routing will make sure that one of the units in the US will call the two other units. This will only result in one transatlantic call. TMS Routing will always find the best way to call between videoconference units, even in large MCU conferences with many partici-pants.
To set up call routing in TMS you have to define:

- Locations – Locations give TMS Routing information on which numbers are dialled from systems that use the location. Information about country codes, area codes, area code rules, gateways and internal calls are set-up in locations.
- Systems – Systems that are added to TMS must be added to a location. TMS will automatically check the settings of the system. Important settings are:
    - ISDN Base-Number – Used for making ISDN calls.
    - H323 Gatekeeper – Used for IP calls and ISDN Gateway calls
    - E164 Alias – Used for IP calls.

Locations

In order for TMS to schedule calls (except unlisted sites) and for TMS Routing to create the best possible routes between systems, the system must be added to a location.

TMS users define a location. A location consists of (only data relevant for routing is mentioned here):

- Local dialling prefix
- Long distance dialling prefix
- Country (to find the country code)
- Area code
- Gateway prefix
- Gateway uses ISDN prefix
- ISDN Default for systems in same location
- Number of digits to use for internal ISDN calls
- Preferred connection type (IP or ISDN) between specific locations

Local dialling prefix

Number to call for accessing an outside line for local calls (calls between systems in the same area code)

Long distance dialling prefix

Number to call for accessing an outside line for long distance calls (calls between systems in different area codes or countries)

Country

The country where the systems are located.

Area Code

The area code where the systems are located.

Gateway prefix

The prefix to use when making calls through a gateway. TMS will allow systems without ISDN-lines to make ISDN calls if the location is set-up with a gateway prefix, and the system is connected to a H323-Gatekeeper. This is typically set to be the auto bandwidth prefix of the gateway being used.

Gateway uses ISDN prefixes

Check this box if the ISDN-gateway must use the same dial-out prefixes the system must use. E.g. if the gateway must also dial a digit to get a long distance line.

ISDN default for systems in same location

TMS gives you the option to prefer ISDN or IP calls to be made between systems within the same location. If this checkbox is checked, TMS will prefer making ISDN calls within the location. If this checkbox is not checked, TMS will prefer to make IP calls.

Number of digits to use for internal ISDN calls

If you do not dial all the digits in the ISDN base number, enter the amount of digits to dial when making calls between systems in the same location. E.g. if your systems have the ISDN base number 5551234, but are only required to dial the last four digits when dialling internally (only 1234), you should enter 4 in this field.

Preferred Routing

The following consideration are taken into account when making calls:

- The maximum allowed participants for Internal and external MCUs – For TANDBERG end-points that have the Multisite option enabled, a maximum of 3 other participants may be added. For a TANDBERG MCU the maximum capacity of the unit can not be exceeded (See TANDBERG MCU documentation for further details).

- Gateway systems – TMS will allow systems only connected by IP to dial other systems using ISDN by going through an ISDN-gateway. TMS will then always initiate the call from the system that need the gateway to dial ISDN.

- Automatic inclusion of external MCU's – If due to the amount of systems selected to call between, an external MCU is required. TMS will automatically allocate an MCU using the same preferred routing as described below.

The preferred route

TMS will weight the factors described below to select a preferred route:

- The available ISDN and IP bandwidth for the systems – If the preferred bandwidth to use for the call is 384 kbps and a system only supports 768, a four site conference using ISDN will not use that internal MCU unless no other MCU is available. The reason is that this would reduce the quality of the meeting (each participant would only use 256 kbps bandwidth and not the preferred 384 kbps)

- Minimum amount of international calls – TMS will prefer making long distance or local calls than making international calls.

- Minimum amount of long distance calls – TMS will prefer making local calls than making long distance calls.

Area code rules

An area code rule determines how ISDN-numbers are dialled from systems registered in the current location, to other area codes within the same country. Area code rules are typically used to handle the following cases in the US dialling plan:

- Area code overlays – Calls between two different area codes are local calls. The calls also require 10-digit dialling.
- Local long distance – Call between the same area code are long distance calls, requiring a long distance prefix to be dialled.

Area code overlays

The normal dialling rule in the US is to dial 7-digit numbers for local calls, and the number one plus a 10-digit number for long distance calls. However some larger cities use area code overlays, which require 10-digit dialling between systems.

Given there is an office situated in New York. This office uses '555' as its area code. The normal dialling rule when dialling between area codes, is that a '1' is included before the area code and the base number, for example 1-555-1234567. The '1' is the long distance prefix. However as New York is a large city, area code overlays are used. Given that New York uses area codes 555, 556 and 557, calls placed between these area codes are local calls. When dialling between these three area codes, you do not use the long distance prefix ('1'). Another requirement is that 10-digits are always used, even when dialling within the same area code. Because of dialling in New York differs from the national dialling rules in the US, we need to define area code rules.

To set-up a location to use area code overlays, you add dialling rules. Given we are setting up the dialling rules for systems located in the 555 area code in our example above, the following area code rules must be added:

• Dialling between 555 and 555 requires that the area code be included, but no long distance prefix is needed.
• Dialling between 555 and 556 requires that the area code be included, but no long distance prefix is needed.
• Dialling between 555 and 557 requires that the area code be included, but no long distance prefix is needed.

The picture above shows how to make one of the area code rules (from area code 555 to area code 556). Additional rules for 555 to 555 and 555 to 557 must be made to complete the example above.

Local long distance

Local long distance is for calls placed between systems located in the same area code. A long distance prefix must be added.

A US number consist of the following parts:

           Area code

X - XXX - XXX -   XXXX

                          Prefix

Given that Smalltown in USA uses local long distance. Smalltown uses the area code 344. Smalltown only uses the prefixes starting with a '3' (e.g. 300, 310, 320 etc), when dialling any other prefixes, long distance dialling is required.

To achieve correct calling for places like Smalltown, the following area code rule must be set for the Smalltown location.

Dialling within the area code 344, with prefixes that start with numbers other than '3', long distance dialling must be used.

Area code rule for Smallville. This rule ensures local long distance within the area code 344 when dialling number that use prefixes starting with numbers other than 3.

Dialling rules that cannot be configured by a TMS user

The following rules are set by TMS by default. A TMS user does not have to be aware of these rules, but to understand the routing logic, it may be worth to mention.

- Long distance rule. Notice: Applies only to long distance calls, does not apply to international calls.
- Same area rule.
- International dialling prefix.

Country Dialling Rules

You can edit country specific dialling rules by selecting the '**Country Dialling Rules**'. Note that this function should only be used by advanced users.

Long distance rule

A number to dial when dialling long distance calls within a country. As an example for the USA, a long distance call is to be placed. The long distance prefix '1' must be added before the area code and the base number of the system.

Same area rule

Defines if the area code is included or not for calls within the same area code. In addition a prefix can be set before a call within the same area code.

International Dialling Prefix: Number to be dialled to call out of a country. In Norway this number is 00.

TMS Watchdogs

The TMS WatchDogs catches SNMP traps and events from the systems in your network. Three TMS WatchDogs are installed during the TMS installation. They are installed as Services to protect the server from unauthorized usage, and will be started after finishing the installation procedure. In the 'Services' console they are marked as '**TMSWatchdogTrapHandler**', '**TMSWatchdogScanner**' and '**TMSWatchdogNetworkScanner**'.

The TMS WatchdogTrapHandler is event driven and receives SNMP traps from systems registred in TMS and process these accordingly. All activities on the systems are registred by the TrapHandler.

The TMS WatchdogScanner polls the systems registred in TMS, i.e. on regular internvals the Scanner will poll the systems registred in TMS to supervise them and consequently update the database entries for these systems. E.g. if a systems for some reason becomes disconnected from the network, the Watchdog Scanner will detect this. The TMS WatchdogScanner sends out SNMP queries to the systems by default every 15 minutes. This values can be changed in the 'Administrative Tools - TMS Configuration - SNMP Scan Interval'.

The TMS WatchdogNetworkScanner continuously scans your network for new systems and adds them into your database. The Networkscanner uses Broadcast to detect systems, and hence requires your network to be broadcast enabled in order to automatically detect new systems. The Network scanner stores all found systems in the database. Note that a system may be stored in the database even if it is not represented in any of the system folders under 'System Management - Navigator' in TMS.

In the 'Administrative Tools - TMS Watchdog' you can get the status of the TMS Watchdog Traphandler, the TMS Watchdog Scanner and the TMS Watchdog Network Scanner. The uptime for these watchdogs will also be displayed. If a service stops, the watchdog will be marked as 'Not Running'. If the Watchdogs are running on another server, the IP address of that server needs to be entered into the 'WatchDog Address' field under 'TMS Configuration' in order to present the status of these.

Watchdog Logs

The events and SNMP traps caught by the Wathdogs are stored in logs that are used by the Event Handler to notify those who subscribe to these types of events and traps, and to provide statistics.

The Log files can be accessed from the '**TMS Watchdog**' menu under '**Administrative Tools**' or it can be found under

        C:\Program Files\TANDBERG\TMS\wwwTMS\ExportFiles\Logs\

The name of the Log is in the format 'TMSWatchdogTraphandler<date>, 'TMSWatchdogScanner<date>.log' and TMSWatchdogNetworkScanner<date>.log. Events such as an error will be logged in these files with a name and a short description of the event. Typically if the WD did not succeed updating a system, could not reach a system by SNMP etc. these log files will tell you what went wrong.

The <date> part of the file name describes the date when WD was started. A new log file will be created daily.

In the 'Watchdog Logs' page the last 10 entries in the TMS Watchdog Traphandler will be displayed. Press 'View todays full log here' to get all today's events listed on the monitor. The last 10 Log files for the Watchdogs is also availlable from this page.

Clean-Up Systems

Clean-up systems allows you to remove and purge system entries from your TMS database that are no longer needed or which you no longer wish to see represented in TMS. Select the systems to purge and press the '**Clean-up System**' button at bottom of the page.

How to make a backup of the database

When TMS is installed, a version of MSDE 2000 is automatically installed on the server (if there is not one there already). Making backups of this database can be done manually, but to make the process more easy TANDBERG offers a tool for making database backups, restoring old databases and purging database records. This tool is called TMS Database Management Utility.

The TMS Database Management Utility tool is included on the TMS CD-Rom (or zip file) and has to be installed on the same server as TMS. A separate installation is needed. The Database Management Utility tool will also work on older versions of TMS, meaning that it also can be used to revert to an old version of TMS (provided an old database backup exists).

Once installed on the TMS server, the tool is located under the 'Start' menu of your TMS server. See '**Start**->**Program**->**TANDBERG**->**TMS Database Management Utility.**

Database Backup, Restore & Purge Utility

Database Backup

To make a backup of your TMS database, open the TMS Database Management Tool, and click on the button for Backup. A window appears with three tabs: Backup Location, History and Automatic Backup.

Backup Location

The Backup Location selects the location where the backup files will be placed. It is recommended to create a new folder for the backup file location.

History

On the History-folder the history drop-down list you can specify the maximum number of backups you wish to store on disk at any one time.

Automatic Backup

Under the Automatic Backup folder you may specify the schedule for automatic database backups. In order for this feature to work, you first need to install the **TMS Database AutoBackup Service** on the server running TMS.

Once you have selected your backup location, history and automatic backup settings, simply press "**Save Settings**" or "**Backup Now**". If you have made changes to the settings and press "**Backup Now**" a message box will appear asking you if you want to save the settings first.

*Note : The TMS Database AutoBack Service can be installed from the Start menu on the server running TMS. See '**Start**->**Program**->**TANDBERG**->**TMS Database AutoBackUp Service**.*

Database Restore

Open the TMS Database Management Tool from , and click on the button for '**Restore**'.

In the pop-up window, select the desired backup file to use (the filename contains a timestamp in the form databasename_yyyymmddhhmmss.bak). Then press the '**Restore**' button and wait for the database to be restored. A message box will appear declaring the result of the restore operation.

Purge Records

All events and records created by TMS are stored in the database. There is currently no mechanism to automatically delete old records from the database, so this has to be done manually. If records are not deleted, the database will continue to grow, and will eventually become very slow.

To purge (remove) records from the database, open the Database Management Tool, click on the button for '**Purge**'.

When the window appears, select the type of log that will have its records purged. Enter a valid date (date must be less than the current day's date) and press the "Purge" button.

After pressing the purge button, a confirmation message box will appear giving details of the purge about to be performed. This includes the number of records that will be purged during this operation and the percentage that the log file will be reduced by after this operation. Click "Yes" to continue with the purge operation or "No" to cancel the purge operation.
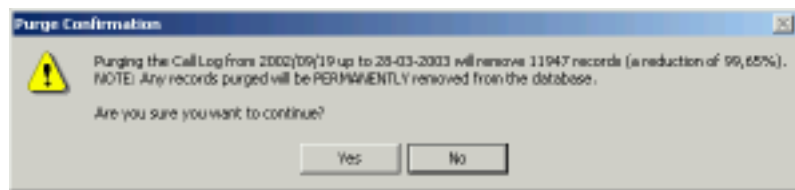
Option: Web Conferencing

About Web and Data Conferencing

Web and data conferencing solutions are important and powerful supplements to video conferencing, providing enhanced collaboration as well as powerful features for voice-only participants.Web and data conferencing enables user to more actively participate in the conference by allowing them to use, show and share applications on their PC with the other meeting participants.

Data Conferencing is a simple and secure way for end users to share their PC screen with the other participants in a conference. All the participants in the conference can take control over the Web Conference and share their PC screen, while the remaining participants can view, point at and annotate on the displayed image.

Web conferencing provide more enhanced features such as viewing, annotation and collaborative text editing of documents as well as application sharing and remote control of an application or a computer.

Integrated Web and Data Conference Booking

TMS offers the option to include web or data conferencing as part of its booking features. While the setup of such a conference can be controlled by TMS, a separate server or service is required for the actual web or data conference to take place.

Supported Web and Data Conference Solutions

TMS has been integrated towards the following web and data Conference Services:

- TANDBERG See & Share data conferencing

- WebEx Interactive Conference Services

TANDBERG See & Share

The TANDBERG See & Share data collaboration software is a client/server application that can be installed on a separate PC in the same network as the TMS server. For more information about TANDBERG See & Share, please refer to the See & Share User's Guide and System Administrator Guide or contact your TANDBERG representative.

WebEx Interactive Conference Services

WebEx is a Service Provider company offering hosted web conferencing services to enterprises world-wide, throught their reliable, secure, global network. To sign up for their services, please contact WebEx directly to establish an account.

For more information about WebEx, please visit *www.webex.com.*

Setting up TMS for Web Conferences

In order to set up web or data conferences using TMS, your TMS server needs to be configured and linked towards your Web Conference Server or Service of choice.

Click on the '**TMS Configuration**' link under '**Administrative Tools**' in the top frame of the window to get access to the configuration page of the TANDBERG Managment Suite. For a more detailed description of all the parameters in this folder, please refer to chapter '*Advanced use - Administrative Tools*'.

TANDBERG See & Share Configuration

To configure TMS to use TANDBERG See & Share for data Conferencing, select the TANDBERG See&Share option in the scroll-down menu in the field named 'Enable Web Conference support'.

TMS Configuration: web conferencing parameters for TANDBERG See&Share

URL for web conferencing server

In the field 'URL for web conferencing server', enter the IP address or the DNS name of the server running TANDBERG See&Share software.

Password for web conferencing server

Enter the password for creating Web Conferences on the TANDBERG See&Share server. This password is set on the TANDBERG See&Share when installing the server, and can also later be changed using the provided Administration tool for the TANDBERG See&Share server .

Click on the '**Update**' button to store your changes.

Please note the '**WebConference connection status**' below the Web Conference parameters. If TMS is able to connect to the TANDBERG See&Share server, this status should read: 'Successfully connected to TANDBERG See&Share server: *<your server>*'.

If the connection is not successful, please verify your parameter settings and check that the TANDBERG See&Share server is running ok.

WebEx Configuration

To configure TMS to use WebEx web conferencing, select the WebEx option in the scroll-down menu in the field named 'Enable Web Conference support'.

TMS Configuration: web conferencing parameters for WebEx

Web Conference URL

Enter the URL address to the WebEx server. This address will be provided to you by WebEx upon signing up for their services.

Password for WebEx Server

Enter the password for creating Web Conferences on the WebEx hosted server. This password will be provided to you by WebEx upon signing up for their services.

UserName for Web Conferencing server

Enter the User name for the WebEx Conferencing Server. This parameter will be provided to you by WebEx upon signing up for their services.

SiteID for web conferencing server

Enter the SiteID for the WebEx Conferencing Server. This parameter will be provided to you by WebEx upon signing up for their services.

PartnerID for web conferencing server

Enter the PartnerID for the WebEx Conferencing Server. This parameter will be provided to you by WebEx upon signing up for their services.

Click on the '**Update**' button to store your changes.

Please note the '**WebConference connection status**' below the Web Conference parameters. If TMS is able to connect to the WebEx Conferencing server, this status should read: 'Successfully connected to WebEx server: http:// www.webex.com/....'.

If the connection is not successful, please verify your parameter settings and check that the WebEx server is running ok.

Booking a Video and Web Conference using TMS

Booking a TANDBERG See&Share data conference

To include a TANDBERG See&Share data conference in a TMS booking is very easily done. When performing the booking, the end user simply ticks off a check-box indicating that See&Share data conference will be used.

Booking a video conference conference with See&Share

The rest of the booking is done just like any other video conference booking. See chapter on '*Advanced Booking*' for futher details.

Note: To book a TANDBERG See&Share data conference, your TMS server must be configured to use an external See&Share server. Please refer to chapter on 'Setting up TMS for Web Conferences' for more information.

Booking a WebEx conference

To include a WebEx conference in a TMS conference booking is done very much the same way as with TANDBERG See&Share. When performing the booking the end user simply ticks off a check-box indicating that a Web Conference will be used.

Booking a video conference with WebEx

The rest of the booking is done just like any other video conference booking. See chapter on '*Advanced Booking*' for futher details.

Note: To book a WebEx web conference, your TMS server must be configured to use WebEx. Please refer to chapter on 'Setting up TMS for Web Conferences' for more information.

Booking Confirmation Email

Upon completion of the booking, an email confirmation is sent to the person booking the conference. This email contains all necessary information needed for the participants to join in on the conference, including a link to the web or data conference. By forwarding this email to the meeting participants, they only need to click on the provided link to join the web or data conference.
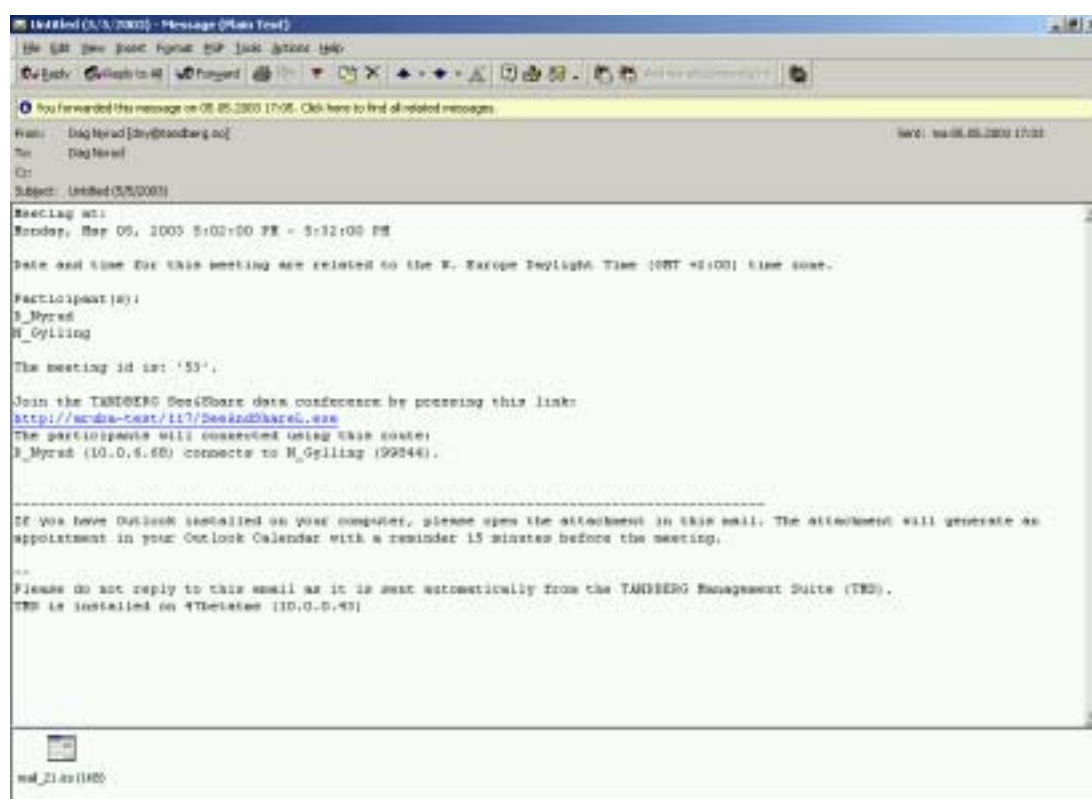
Example of booking confirmation email for a video and data conferece (See&Share)

For more information about using web conferencing, please refer to the User manual of your web conference solution.

Option: Microsoft Exchange Integration

TANDBERG offers an optional component to fully integrate the TANDBERG Management Suite (TMS) with Microsoft Exchange and Outlook. This integration gives the users the ability to schedule videoconferences, book meeting rooms and invite participants using their Microsoft Outlook client.

The videoconferencing systems are registered as resources in Exchange, allowing end users to view their availability when making the booking.

The integration requires a software component to be installed on the Microsoft Exchange server.
Note that there is no need to update any of the Microsoft Outlook clients.

PLEASE NOTE: INSTALLING COMPONENTS INTO MICROSOFT EXCHANGE SERVER REQUIRES A DEEP AND THOROUGH UNDERSTANDING OF MICROSOFT EXCHANGE. IT IS NOT RECOMMENDED TO COMMENCE THIS INSTALLATION WITHOUT THE SUPPORT AND PRESENCE OF A MICROSOFT EXCHANGE EXPERT.

Please see www.microsoft.com for more information about Microsoft Exchange.

Server Requirements

In addition to the Exchange requirements(please refer to the Software Requirements chapter), the TMS Exchange Integration component requires additional CPU and memory on the Exchange Server.

It is recommended to use minimum a 1 GHz server for the TMS Exchange Integration component, with at least 512 MB RAM. This depends on the number of users.

Software requirements

The TMS Exchange Integration component supports:

Microsoft Exchange 2000 with Microsoft Exchange service pack 3 installed on a Microsoft Windows 2000 server with service pack 3. Exchange System manager must be installed.

Microsoft Exchange 2003 installed on a Microsoft Windows 2003 server.

On the client side, Microsoft Outlook 2000, Microsoft Outlook 2002 and Microsoft Outlook 2003 is supported.

Limitations

Only one Exchange server can connect to TMS in one AD domain. If there are multiple domains that are integrated with the same or different TMS server(s) (in one forest), it is recommended to hide the resources between the domains. TMS will not correctly build a call route if the resources are split between domains.

All resource accounts representing Videoconference systems in one TMS Exchange Integration must have mail boxes on the same Exchange server. They will however be accessible to all users in the same exchange organisation.

Installation

Before you start installing the TMS Exchange Integration component on the Exchange server, make sure you are logged in as a user with local, domain and full Exchange administrator rights.

Close all other applications running on the server.

Download the TMS Exchange Integration software package to the server (or insert the CD ROM into your CD ROM drive), and start the installation program (setup.exe) for the TMS Exchange Integration.

The installer will search for an already installed version of the TMS Exchange Integration component. If one is present, the installer will start the uninstall wizard before commencing the installation of the new component.

The installer will automatically install the TMS Exchange Integration component.

Note: The installation of the TMS Exchange component may require the installation of the additional Windows components (Windows component update). If this is the case, the installation will terminate and ask you to install these components. The Windows component update is supplied as a separate installation, included on the TMS CD-Rom. Install the Windows component update (may require a restart of the server) and then start the TMS Exchange Integration again.

1. The TANDBERG installer will prepare the installation wizard.
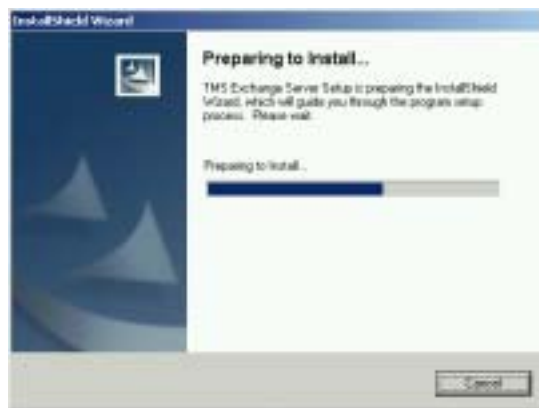
2. A welcome window will appear on the screen. Press the '**Next**' button.

3. Read and accept the License Agreement.

4. Select the destination folder where Setup will install the files. Click '**Next**' to accept the suggested path, or '**Browse**' to change the path.
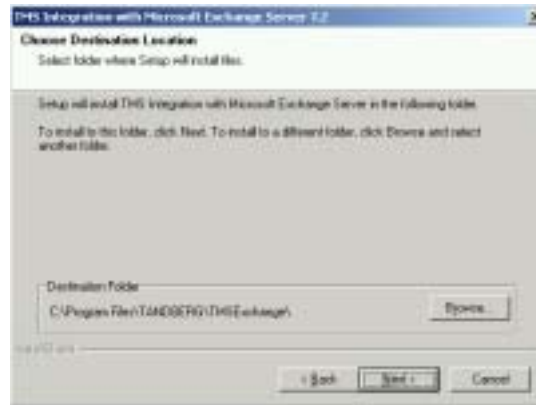
5. The installer will create a service account with a mailbox on the Exchange server. Select which store on the Exchange server you would like to use from the scroll-down menu, and click '**Next**'.

6. Enter the IP address or host name of the TMS server, and the user name and password to an account that has at least local computer admin rights on the TMS server **and** Site administrator rights in TMS.

Note: The Exchange server needs to be able to reach port 80/HTTP on the TMS server(in case of firewall issues).

7. The Exchange Integration will create 3 security groups in the domain. Press the 'Next' button to accept the default values suggested by the installation wizard.

Note: Videoconferencing endpoints in TMS need to be registered as resource users in Exchange and will be put in the first group. Users in your organization that should have access to booking of videoconferences using Exchange/Outlook should be granted access to the second group, while admins should be granted access to the third group.

8. The next page allows you to put all the TMS-Exchange integration users and groups in a separate container in Active Directory. If you want to put them under an Organizational Unit (or create a new Organizational Unit), click on the '**Browse AD**' button. Otherwise click on the '**Next**' button.

Note: Post-install moving of the users and groups to a different Active Directory Container/organizational unit through "Active Directory Users and Computers" is not supported.

9. If you clicked on the '**Browse AD**' button you can specify which Organizational Unit to use, or create a new Organiszational Unit.

10.Confirm the settings defined in the installation process and select '**Next**' to start copying files.

11. Press FINISH to complete the installation.
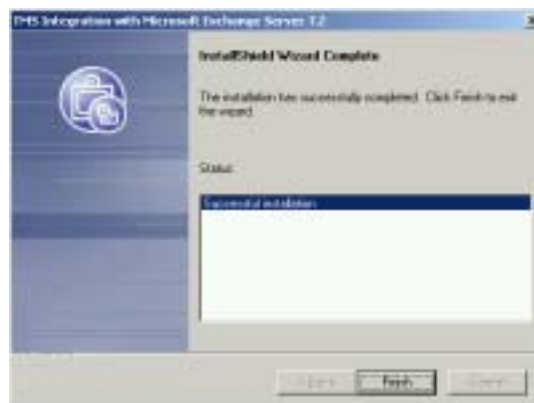
Notes about the Exchange installation

In order to perform, supervise and synchronize all the bookings between Exchange an TMS, the installation of the Exchange component causes 2 user-accounts to be created.

In the domain where the exchange server resides, a user 'tms-service' is created. On the user database of the TMS server, a user account 'tmsconfuser' is created.

Uninstall TMS Exchange Integration

Run 'setup.exe' again to uninstall the TMS Exchange Integration component from the Exchange Server or use use 'Add/Remove programs' from the Control Panel of the server.

The unistall procedure will remove the user representation created during the install procedure as well as the address list created for the videoconference systems.

Post Installation Setup

Once the TMS Exchange Integration component is installed on the Exchange server, three important steps need to be done in order to make the installation complete.

>   1 - Publish the provided VideoConference form.
>   2 - Create Exchange User representations for each system registered in TMS
>   3 - Start Synchronizer to import existing TMS booking entries for videoconference systems

Publish the provided VideoConference Form.

A custom appointment form that adds support for videoconference meetings is provided as part of the release from TANDBERG. It is recommended to place this form under Organization Forms Library in order to be made available for all the Exchange end-users in your network. If an Organizational Forms Library already exists on your Exchange server, this one can be used (make sure permissions are set as described in the following chapter). If not, one has to be created before importing the custom form. Please see www.microsoft.com/exchange for more information about Microsoft Exchange.

Creating Organization Forms Library

Be sure you are logged in with full Exchange administrator rights. Go to '**Administrative Groups**' and then select the group containing the Exchange Server on which you just installed the Exchange Integration component. Normally this would be 'Administrative Groups/First Administrative Group'.

Select '**Folders**' followed by '**Public Folder**'. Right-click on '**Public Folder**' and select '**View System Folders**'.

Note: 'Folders' may reside on root level if the Exchange System Manger is not configured to show administrative groups.

While viewing the System Folders, right-click on '**EFORMS Registry**' and select '**New**->**Organizational Form**'
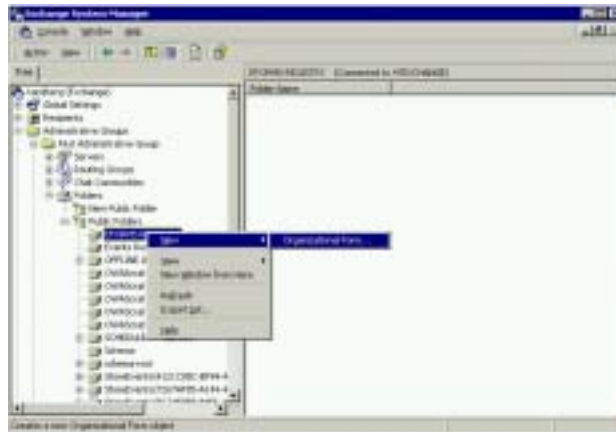
A template for the new Organizational Form will be displayed. Fill in a suitable name and (optional) description of the Organizational Forms Library. Choose 'English (USA) as E-forms language.

Press '**OK**' to save Organizational Forms Library.

In order to put the VideoConference form in the Organizational Forms Library, an Outlook user needs to be granted "owner" permissions to the Organizational Forms Library. It is recommended only to give one single end user the 'owner' permission (preferably an administrator) , and use this users for publishing the form.

This is done by right-clicking on the created folder, select '**Properties**'. In the pop-up window, select the '**Permissions**' page.

Click on the '**Client Permission**' button to change and review permissions for the Organizational Forms Library.

Note that the permission level must be '**owner**' in order to publish into the library.

Publish Custom Form

Once the Organizational Forms Library is in place, the Custom Form provided by TANDBERG can be placed here. As this has to be done from an Outlook client, you need to log on to the mailbox of a user with "owner" permissions to the Organizational Forms Library (permission levels set as described above).

On the PC where Outlook is running, open the **videoconference.oft** file provided by TANDBERG.

The file is located where the Exchange Integration component was installed. If you have admin rights to the exchange server and the default path was not changed during installation, this would be:

\\<exchange server name>\C$\Program Files\TANDBERG\TMSExchange\Video Conference Form\ videoconference.oft

Copy the file to a diskette or CD-ROM or use a network store to run it on the PC where Outlook is running.

Opening this file will cause the following screen to appear. To publish the form, select '**Tools->Forms->Publish Forms as ...**', as shown in the picture below.
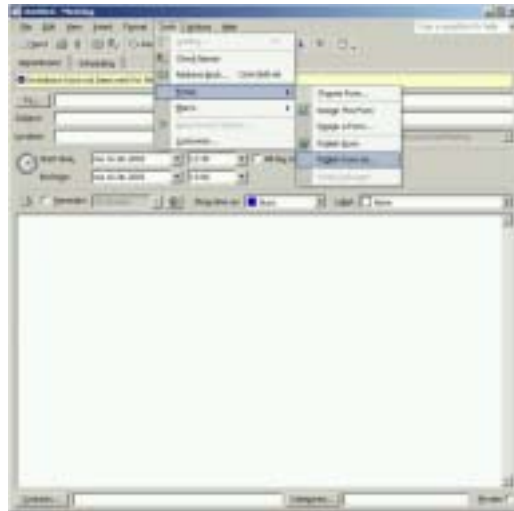
A screen for publishing the form will then pop up.

It is important that the fields are filled in exactly as described below (case sensitive).

> Look in: select **Organizational Forms Library**
>
> Display name: enter '**Meeting**'
>
> Form name: enter '**VideoConference**'

Note: 'Form Name' is case sensitive and must be entered exactly as described above.

Press '**Publish**' when done.

You have now completed step 1 (out of 3) of the post installation process.

Create Exchange User representations for each system registered in TMS

Each videoconferencing system that you want to be able to book and use from Exchange/Outlook needs a representation in Exchange. This representation is done by adding a 'User' in Exchange for each of the videoconferencing systems.

The user representation for these systems must be set up in a particular manner, and in order to simplify this process, TANDBERG provides a tool to assist in the creation of these users.

This tool can be found on the Exchange server on which the TMS Exchange Integration component was installed. Under the '**Start**' menu, '**Programs**' -> '**TANDBERG**' -> you will find '**Exchange Integration Init**'

Make sure that you have administrator rights (to create users) on the Exchange server, and start the provided tool on the Exchange Server.
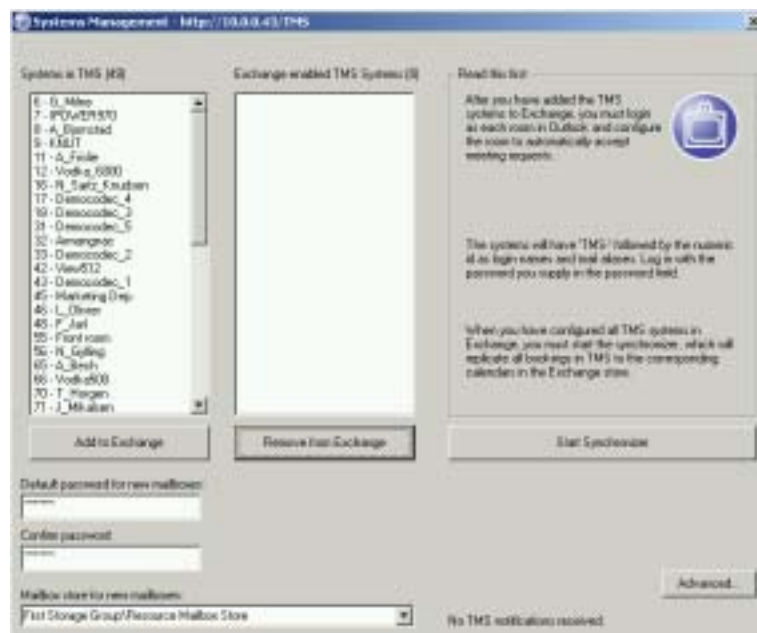
Note: The user accounts created in Exchange representing the videoconferencing systems do not require any licenses from Exchange. Exchange licenses are tied up against the number of Outlook installations accessing the Exchange server. So, accessing lots of different user-accounts through your Outlook client still only uses 1 license.

The tool will automatically fetch information about all videoconference systems from TMS and present them on the left hand side of the screen.

Fill in the '**Default password for mailboxes**'. All the user accounts created using his tool will have this password.

Highlight each of the systems you want registered in Exchange, and select the '**Add to Exchange**' button. The system will then be moved over to the column '**Exchange enabled TMS Systems**'.

For each system that you 'Enable', a user account with the name tms-'system id' is created (e.g. from the previous picture, the following users are created: tms-6, tms-7, tms-8 etc.). The number in front of the system name in the systems management tool is the system id.

The message '**No TMS notifications received**' indicates that the Exchange Integration component has not received any events from the TMS server. This is normal if no bookings have been performed in TMS since the installation of the Exchange component completed. If this message is still present after usage of TMS, this indicates that the TMS server can not send emails to the TMS-Service User in the Exchange domain. This will cause a delay in the synchronisation process from TMS to Exchange. Please contact you email administrator to verify that the SMTP server specified in TMS is configured to deliver emails to the Exchange domain.

The '**Advanced**' button allows you to change the password for the tms-service account created on the Exchange server. You can also change the log path, rebuild the TMS server connection and select options for Asynchronous meeting requests.
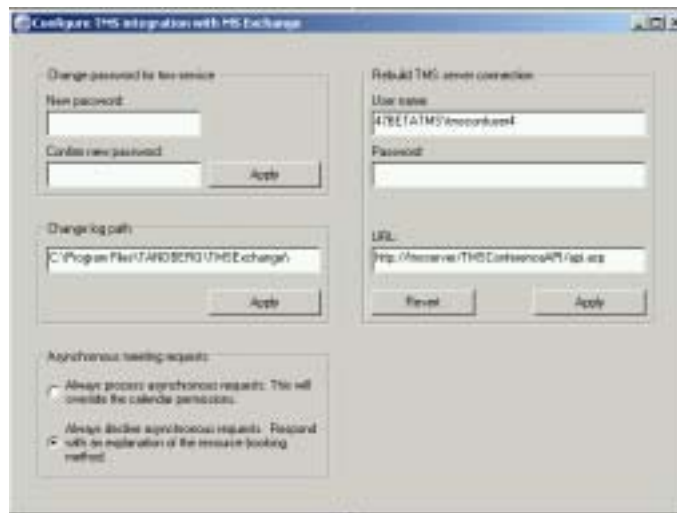
Automatic acceptance of meeting requests

When creating the user account representing the videoconference systems, the Exchange Integration Init tool will try to set all the accounts to automatically accept meeting request. This is required inorder to be able to book them as resources.

However, in some Exchange environments the tool may not be able to set this parameter (for many reasons). If this should happen, an indication in the response message received after clicking the '**Add to Exchange**' button will be given for the account in question.

You then need to manually set this parameter for each account by logging into the mailboxes through Outlook.

To do this, you need to logon as each user representing the different videoconferencing system, using user names and passwords created by the above-mentioned tool.

*Note: It is recommended to add a new profile and set '**Logon Network Security**' to '**None**' when logging on as another user. Setting 'Logon Network Security' to 'None' implies that Outlook will not use your NT logon information when Outlook is opened, but will prompt you for username and password. This way, you only need to restart Outlook to change to a different user instead of logging completely off your PC.*

*To change Network Logon Security, right click on your Outlook icon and select '**Properties**'.Click on the '**Show Profiles**' button and select the Exchange profile you are using. Click on '**Properties**' for this profile and then select '**Properties**' again for the Microsoft Exchange Server. Under the '**Advanced**' folder, you will find a field called '**Logon Network Security**'. Set this parameter to '**None**' and click '**OK**' on all the pop-up windows.*

In Outlook, select 'Tools' -> 'Options'.

Under '**Preferences**' select the '**Calendar Options**' button.
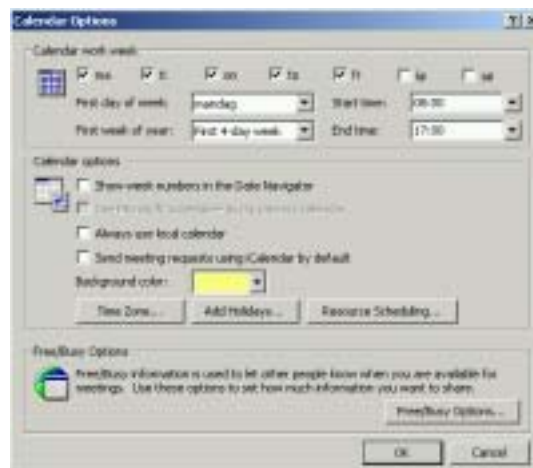
Select the '**Resource Scheduling**' button.

Tick off the 'Automatically accept meeting request and process cancellations' and press 'OK'. If you are asked about setting default permissions when clicking "OK" then do so! Even if you want to change the permissions later.

Customize Calendar permissions

If you would like to customize the calendar permissions, you can right-click on the calendar folder icon in the "Folder List" pane and click "Properties".

In the "Calendar Properties" page that pops up, switch to the "Permissions" tab page.

Authors can book and edit/delete their own bookings, Editors can book and edit/delete all bookings.

You have now completed the second step (out of 3) of the post installation process.

Import existing TMS booking entries for videoconference systems

In the previously mentioned tool, TANDBERG has included a feature to import existing bookings in TMS into the calendar representations of the videoconferencing systems in Exchange.

It is therefore recommended that you 'Enable' all your TMS systems in Exchange before doing this operation. When later adding new systems to TMS, it is recommended to enable them in Exchange before you start using them from TMS.

The operation is simply done by pressing the '**Start Synchronizer**' button on the Exchange Integration Init.
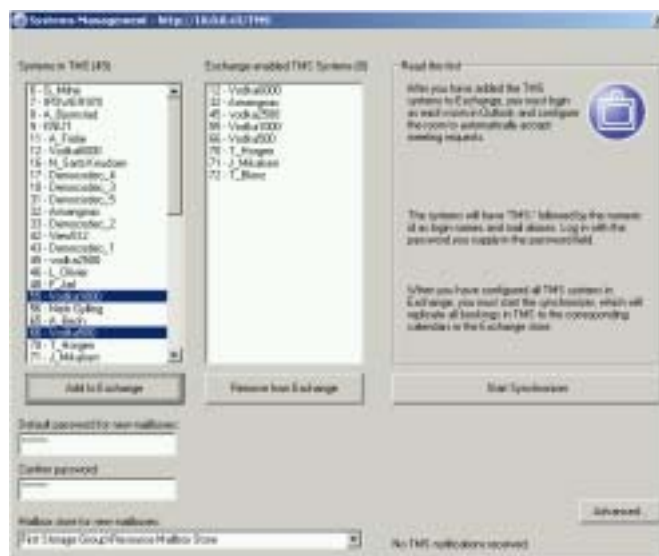
A confirm message will pop up and give a warning that this operation only can be done once. Press '**Yes**' to confirm the synchronization.

All existing meetings in TMS will now be imported into the videoconference systems representation in Exchange.

The post installation process is now completed (step 3 out of 3), and you are now ready to start booking videoconferences using Exchange.

Note: Personal calendars are not updated if changes are made through TMS. When changes are done in TMS, the resources' calendars are updated, while the organizer will receive an e-mail from TMS about the update.

Making a booking using Outlook

Activating VideoConference Form

Before an end-user can start booking videoconferencing rooms using Outlook, each user must have the new Videoconference form activated on their Outlook.

You can change the default form in Outlook by making changes to the Microsoft Windows Registry. The registry settings specify which forms are substituted for the default Outlook forms. An Exchange administrator can change this registry entry for all users using login scripts. Please refer to article Q295064 in Microsoft Knowledgebase for further information (See http://support.microsoft.com/default.aspx?scid=KB;EN-US;q295064&ID=KB;EN-US;q295064).

The form can also be activated manually by each individual user from their Outlook client:

Right-click the Calendar icon on the user's Outlook, and select '**Properties**'.

Under the '**General**' page select '**Forms..**' from the scroll down menu next to '**When posting to this folder, use:**'.

In the pop-up window, select '**Organizational Forms Library**' from the scroll down menu at the top (under '**Look in**'), and double click on the posted form called '**Meeting**' (if you used the naming convention proposed in the installation guide).
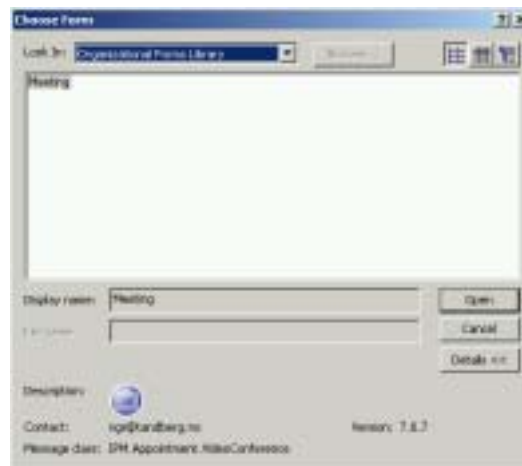
Booking meetings with Videoconferencing rooms

Booking your videoconference meeting can now be done in the same way as an ordinary meeting room/resource booking in Outlook. When adding videoconferece systems to the meeting, these can be found in the 'VideoConference Rooms ' address book. It is recommended to add each videoconference system as **Resource** to the meeting. Select all the videoconference systems and users you want to participate in your meeting.

Note: By adding videoconference rooms as 'Resource', Outlook will try to book the the meeting directly in the calendar of the videoconference system before the meeting invitation is sent to the meeting participants. By adding them in the same way as regular participants ('Required'), you will get the confirm/reject message per email later.

Under the 'Attendee Availability' folder of your meeting request you will see the free/busy overview of all the participants in your meeting, including the videoconference systems. This will assist you locating a suitable time for your meeting.
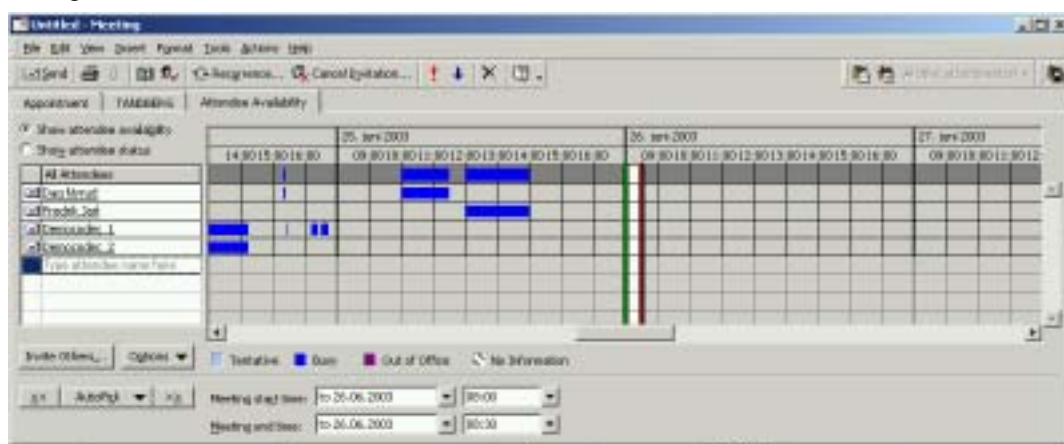
Once you add a videoconference system as a resource in your meeting, you will notice that your meeting request now has been expanded to include a '**TANDBERG**' page. Under this page, you will be presented with more detailed information about the videoconference. Here you will also be allowed to set some additional parameters for your videoconference as well as inviting external participants.
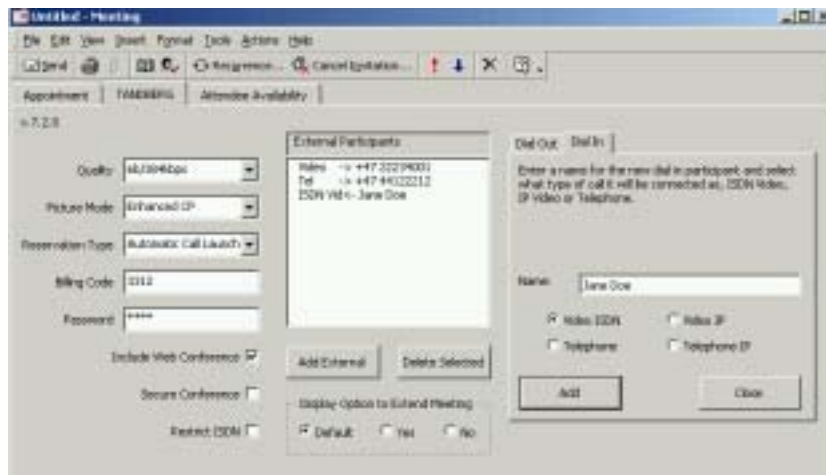
The following parameters and functions are available from the TANDBERG folder of you meeting request:

Quality

Defines the quality of the videoconference call, i.e. the requested bandwidth. If set to '**Default**', the default bandwidth defined in TMS will be used.

Picture Mode

Defines the screen layout for multipoint conferences. Options are '**Enhanced CP**', '**Continuous Presence**', '**Voice Switched**' and '**Default**'. If set to '**Default**', the default value defined in TMS will be used.

Reservation Type

The reservation type parameter indicates what kind of reservation this is. The default value is configured in TMS. Setting this parameter to '**Automatic call launch**' will cause the video conference to be set up automatically when the meeting is due. Setting lauch type to 'Manual Call launch' requires an end user to confirm the call setup from each of the endpoint before the call is initiated.

Billing code

This field allows you to enter the billing code which shall be used for the booking. See chapter on '**Billing Codes**' under '**Advanced use**' for futher details.

Password

This field allows you to assign a password to the conference. Participants calling in to the conference will have to enter this password to be able to join the conference.

Include Web Conference

Enables a web or data conference to be booked with the meeting. See chapter on '**Web Conference**' for further details.

Secure Conference

Enables secure conferences by encrypting the videoconference call.

Restrict ISDN

Allows you to specify if the conference should call restrict (56kbps) or not.

Display Option to Extend Meeting

Allows you to specify if the conference master should be presented with the option to extend the meeting using the quick keys on his remote control.

Add External

By pressing the '**Add External'** button, a pop-up window will allow you to add external dial-in or dial-out participants.

For Dial-Out participants, i.e. participant that will be dialled up by TMS, enter the phone number they are reachable at and specify what kind of equipment that shall be used. Options here are '**Video ISDN**', '**Video IP**' , '**Telephone**', or '**IP Telephone**'. Press the '**Add**' button when done entering information about a participant.

For Dial-In participants, select the 'Dial-In' folder in the pop-up window and enter a reference name for the participant. Also select the kind of equipment that will be used when calling in. Options are the same as for Dial-Out. Press the '**Add**' button when done entering information about a participant. Resources will be set aside for these participants to dial into the videoconference.

You can also delete selected dial-in or dial-out participants by selecting them and pressing the '**Delete Selection**' button.

Send Exchange meeting invitation

When you are done entering all the needed information into your meeting request, press the 'Send' button on the meeting invitation. Exchange will now contact the TMS server and try to book the requested videoconference system at the given time. If the booking is successful, a pop-up window will be displayed.

Changing or editing an existing meeting

Meetings booked using MS Exchange can easily be changed later. Using your Outlook calendar, you can open up the meeting representation in your calendar and do what-ever changes you want to the meeting, for example adding or removing participants, changing the time/date etc. When done with your changes, simply press the '**Send Update**' button to update the calendar entries of all the participants in Exchange and update the videoconference booking in TMS.

The meeting can also be changed from TMS Scheduler or TMS Booking. If you login to TMS and select '**My Meetings**' under the '**Booking**' folder, you will see a representation of your meeting booked from Exchange. You can edit this meeting like any other of your meeting in TMS. Any changes to it will be correlated into the Exchange representation of this meeting and all the systems involved. This way, TMS and Exchange will remain in synchronization all the time.

For more information about booking meetings using Exchange, please refer to www.microsoft.com.

Note: it may take a couple of minutes before Exchange is updated with changes done to meetings from TMS. The other way round happens immediately.

Multivendor Support in TMS

This chapter gives an overview of the level of support provided by the TANDBERG Management System (TMS) for TANDBERG and 3rd party videoconferencing products. The level of support described in this document is related to the latest available release of the videoconferencing products at the release date of TMS.

The level of support for each videoconferencing product is described in separate chapters, including any configuration or set-up details required in order to make the product work with TMS.

The level of support is related to version 8.0 of TMS.

Description of table

For each videoconferencing product described in this document, a table will be presented giving an overview of the level of support provided by TMS. This chapter gives an explanation to the different fields presented in this table.

	Explanation
Basic Monitoring	
Auto Detection, Status ('No Response' or 'Alive'):	Indicates that TMS is capable of automatically detecting the unit in the network and supervising if it is alive or not.
Access to internal web, ftp or telnet (if available):	Indicates that the system's telnet, ftp or web site is accessible from TMS
Scheduling	
Dial Out	Indicates that the system can be booked and scheduled by TMS. The system can both receive calls as well as being told to initiate an outgoing call.
Dial in	Indicates that the system can be booked and scheduled by TMS. The system can only be called (i.e. dial out not possible)

Explanation

Advanced Monitoring

Call Status: Indicates that TMS is capable of detecting the call
                                                status of the system (i.e. if it is in a call or not).

Call Logs: Indicates that TMS is capable of storing call logs (i.e.
                                                call statistics) for the unit, including call attempts and
                                                failed calls.

Graphical Call Monitoring: Indicates that TMS is capable of presenting the call
                                                connections (active calls) between this system and the
                                                other participants of the conference.

System Management

Upgrade   Indicates that it is possible to do a software upgrade on
                                                the system from TMS.

Templates   Indicates that it is possible to download templates (a
                                                specific set of settings) stored in TMS to the system

Settings Backup   Indicates that settings on the system can be stored
                                                (backed up) on TMS. Settings stored in TMS can then
                                                later be restored on the unit.

Phone Book   Indicates that the TMS Phone Book can be used from
                                                the system.

Intelligent Diagnostics   Indicates that TMS can provide diagnostics to ensure
                                                optimal performance of the system towards TMS.

Network Monitoring   Indicates that TMS stores endpoint and network
                                                activities involving the system (trap logs, boot logs)

View System Settings   List of system settings that TMS is able to present
                                                (view settings)

Change System Settings   List of system settings that can be edited from TMS
                                                (change settings)

TANDBERG Endpoints (non-vision series)

Supported versions

Supports version B3 and newer, but TANDBERG recommends software B5 or newer on the endpoints. For full functionality customers should always have latest software, currently B7/E2

Overview

Basic Monitoring

Auto Detection, Status ('No Response' or 'Alive'):	Yes
Access to internal web, ftp or telnet (if available):	Yes

Scheduling

Dial Out	Yes
Dial in	Yes

Advanced Monitoring

Call Status:	Yes
Call Logs:	Yes
Graphical Call Monitoring:	Yes

System Management

Upgrade	Yes
Templates	Yes
Settings Backup	Yes
Phone Book	Yes
Intelligent Diagnostics	Yes
Network Monitoring	Yes
View System Settings	All TMS supported settings
Change System Settings	All TMS supported settings

Setup

SNMP Community Name must be set to one of the Community Names known by TMS.
See Administrative Tools – TMS Configuration - System Interfaces - SNMP Community Name. Other required settings will be discovered by Intelligent Diagnostics when adding system to TMS. Must have telnet, www, and FTP enabled on the codec and across the network.

Must have Telnet, www and FTP enabled on the codec and across the network.

Firewall requirements: SNMP, SNMP Traps, WWW, Telnet, FTP, Telnet-Challenge (Optional).

Limitations/Notes

None

TANDBERG Vision Series Endpoints

Supported versions

Level of support related to release C4 only.

Overview

Basic Monitoring

Auto Detection, Status ('No Response' or 'Alive'):	Yes
Access to internal web, ftp or telnet (if available):	Yes

Scheduling

Dial Out	Yes
Dial in	Yes

Advanced Monitoring

Call Status:	Yes
Call Logs:	Yes
Graphical Call Monitoring:	Yes

System Management

Upgrade	No
Templates	No
Settings Backup	No
Phone Book	No
Intelligent Diagnostics	Yes
Network Monitoring	Yes
View System Settings	Limited
Change System Settings	None

Setup

SNMP Community Name must be set to one of the Community Names known by TMS.
See Administrative Tools – TMS Configuration - System Interfaces - SNMP Community Name. Other required settings will be discovered by Intelligent Diagnostics when adding system to TMS.

Must have Telnet, www and FTP enabled on the codec and across the network.

Firewall requirements: SNMP, SNMP Traps, WWW, Telnet, FTP, Telnet-Challenge (Optional).

Limitations/Notes

Statistics Support limited by events supported by endpoint

TANDBERG MCU

Supported versions

All versions, but TANDBERG recommends software D2 or newer on the MCU.

Overview

Basic Monitoring

Auto Detection, Status ('No Response' or 'Alive'):   Yes
Access to internal web, ftp or telnet (if available):   Yes

Scheduling

Dial Out   Yes
Dial in   Yes

Advanced Monitoring

Call Status: Yes
Call Logs: Yes
Graphical Call Monitoring: Yes

System Management

Upgrade   Yes
Templates   Yes
Settings Backup   Yes
Phone Book   Yes
Intelligent Diagnostics   Yes
Network Monitoring   Yes
View System Settings   All TMS supported settings
Change System Settings   All TMS supported settings

Setup

SNMP Community Name must be set to one of the Community Names known by TMS.
See Administrative Tools – TMS Configuration - System Interfaces - SNMP Community Name. Other required settings will be discovered by Intelligent Diagnostics when adding system to TMS.

Limitations/Notes

Software version D3 or newer on the MCU requires TMS version 7.2 for full functional support. Older versions of TMS will not be able to retrieve ISDN settings from unit or set up cascaded calls correctly.

Must have Telnet, www and FTP enabled on the MCU, and across the network.

Firewall requirements: SNMP, SNMP Traps, WWW, Telnet, FTP.

TANDBERG Gateway

Supported versions

All versions, but TANDBERG recommends software G2 or newer on the gateway.

Overview

Basic Monitoring
Auto Detection, Status ('No Response' or 'Alive'):   Yes
Access to internal web, ftp or telnet (if available):   Yes

Scheduling
Dial Out   N/A
Dial in   N/A

Advanced Monitoring

Call Status: Yes
Call Logs: Yes
Graphical Call Monitoring: Yes

System Management

Upgrade   Yes
Templates   Yes
Settings Backup   Yes
Phone Book   Yes
Intelligent Diagnostics   Yes
Network Monitoring   Yes
View System Settings   All TMS supported settings
Change System Settings   All TMS supported settings

Setup

SNMP Community Name must be set to one of the Community Names known by TMS. See Administrative Tools – TMS Configuration - System Interfaces - SNMP Community Name. Other required settings will be discovered by Intelligent Diagnostics when adding system to TMS.

Must have Telnet, www and FTP enabled on the GW and across the network.

Firewall requirements: SNMP, SNMP Traps, WWW, Telnet, FTP.

Limitations/Notes

None

Polycom ViewStation 128, SP, MP

Supported versions

Level of support related to release 7.2.4 of the Polycom ViewStation 128, SP and MP

Overview

Basic Monitoring

Auto Detection, Status ('No Response' or 'Alive'):	Yes
Access to internal web, ftp or telnet (if available):	Yes

Scheduling

Dial Out	Yes
Dial in	Yes

Advanced Monitoring

Call Status:	Yes
Call Logs:	Yes
Graphical Call Monitoring:	Yes

System Management

Upgrade	Yes
Templates	No
Settings Backup	Yes
Phone Book	Yes
Intelligent Diagnostics	Yes
Network Monitoring	Yes
View System Settings	Hardware Serial No, Software Version, GK address, GK Mode, ISDN No, E164 Alias, Access Code required, Traphost address, Max IP and ISDN bandwidth, MAC address, Uptime, Call info, Management URLs, Language settings Volume, Auto-answer mode, SNMP Contact and Location, System Name
Change System Settings	System Name, SNMP Traphost address, SNMP Community Name, E164 Alias, Volume, Auto-answer mode, SNMP Contact and Location

N/A - Not Applicable

Setup

In order for TMS to support the Polycom ViewStation, the GlobalManagement on the ViewStation must be enabled. This is done by entering the TMS server IP address in one of the 'Management URL' fields on the ViewStation.

After adding the TMS IP address to the list, the system will automatically fill out the rest of the URL (/pwx/ vs_status.asp). The whole correct URL to the TMS server will then appear as e.g. *10.0.0.10/pwx/ vs_status.asp*

SNMP Community Name must be set to one of the Community Names known by TMS. See Administrative Tools – TMS Configuration - System Interfaces - SNMP Community Name. Other required settings will be discovered by Intelligent Diagnostics when adding system to TMS.

The Polycom global Address Settings must also be configured for Phone Books to work.

Must have Telnet, www and FTP enabled on the codec and across the network.

Firewall requirements: SNMP, SNMP Traps, WWW, Telnet, FTP.

Limitations/Notes

After setting password on the system, it needs to be rebooted in order to function properly with TMS.

Autoanswer mode is only supported on point-to-point calls, no auto answer mode for multipoint.

Auto answer mode when "Do Not Disturb" is activated is not supported.

On the Call Status page for a ViewStation in TMS, call duration for current calls are not presented, as this is not reported by the Polycom Viewstations. Call log duration for completed calls are however reported.

It is not possible to compare system settings on the endpoint with the settings stored in TMS.

Due to a bug in the Polycom FX 5.1 software TMS no longer supports dialling and disconnecting pure phone calls (POTS) on the Viewstations.

Statistics Support limited to events supported by the endpoint.

Polycom ViewStation EX, FX, VS4000

Supported versions

Level of support related to release 5.1 of the Polycom ViewStation EX, FX and VS4000

Overview

Basic Monitoring

Auto Detection, Status ('No Response' or 'Alive'):	Yes
Access to internal web, ftp or telnet (if available):	Yes

Scheduling

Dial Out	Yes
Dial in	Yes

Advanced Monitoring

Call Status:	Yes
Call Logs:	Yes
Graphical Call Monitoring:	Yes

System Management

Upgrade	Yes
Templates	No
Settings Backup	Yes
Phone Book	Yes
Intelligent Diagnostics	Yes
Network Monitoring	Yes
View System Settings	Hardware Serial No, Software Version, GK address, GK Mode, ISDN No, E164 Alias, Access Code required, Traphost address, Max IP and ISDN bandwidth, MAC address, Uptime, Call info, Management URLs, Language settings Volume, Auto-answer mode, SNMP Contact and Location, System Name
Change System Settings	System Name, SNMP Traphost address, SNMP Community Name, E164 Alias, Volume, Auto-answer mode, SNMP Contact and Location

N/A - Not Applicable

Setup

In order for TMS to support the Polycom ViewStation, the GlobalManagement on the ViewStation must be enabled. This is done by entering the TMS server IP address in one of the 'Management URL' fields on the ViewStation. This field will then automatically be updated to 'http://tmsserver/pwx'.

After adding the TMS IP address to the list, the system will automatically fill out the rest of the URL (/pwx/ vs_status.asp). The whole correct URL to the TMS server will then appear as e.g. *10.0.0.10/pwx/ vs_status.asp*

SNMP Community Name must be set to one of the Community Names known by TMS. See Administrative Tools – TMS Configuration - System Interfaces - SNMP Community Name. Other required settings will be discovered by Intelligent Diagnostics when adding system to TMS.

The Polycom global Address Settings must also be configured for Phone Books to work.

Must have Telnet, www and FTP enabled on the codec and across the network.

Firewall requirements: SNMP, SNMP Traps, WWW, Telnet, FTP.

Limitations

Local directories on ViewStations FXs are not supported (not supported by Polycom).

Local Address book no longer supported on Polycom Viewstations running software version 5.0 and newer. This is due to a documented change in their software.

From Polycoms homepage:

"System compatibility:
*Please be aware that the Address Book Maintenance Utility is **NOT** compatible with*
Global Management System (GMS), ViewStation EX 5.0, ViewStation FX 5.0 and VS4000 5.0."

Auto answer mode is only supported on point-to-point calls, no auto answer mode for multipoint.

Auto answer mode when "Do Not Disturb" is activated is not supported.

On the Call Status page for a ViewStation in TMS, call duration for current calls are not presented, as this is not reported by the Polycom Viewstations. Call log duration for completed calls are however reported.

It is not possible to compare system settings on the endpoint with the settings stored in TMS.

Due to a bug in the Polycom FX 5.1 software TMS no longer supports dialling and disconnecting pure phone calls (POTS) on the Viewstations.

Polycom VSX 7000

Supported versions

Level of support related to release 5.1 of the Polycom VSX 7000

Overview

Basic Monitoring

Auto Detection, Status ('No Response' or 'Alive'):	No
Access to internal web, ftp or telnet (if available):	Yes

Scheduling

Dial Out	No
Dial in	Yes

Advanced Monitoring

Call Status:	No
Call Logs:	No
Graphical Call Monitoring:	Yes

System Management

Upgrade	No
Templates	No
Settings Backup	Yes
Phone Book	No
Intelligent Diagnostics	Yes
Network Monitoring	Yes
View System Settings	Limited
Change System Settings	No

N/A - Not Applicable

Setup

In order for TMS to support the Polycom ViewStation, the GlobalManagement on the VSX 7000 must be enabled. This is done by entering the TMS server IP address in one of the 'Management URL' fields on the system. This field will then automatically be updated to 'http://tmsserver/pwx'.

After adding the TMS IP address to the list, the system will automatically fill out the rest of the URL (/pwx/ vs_status.asp). The whole correct URL to the TMS server will then appear as e.g. *10.0.0.10/pwx/ vs_status.asp*

Limitations

At time of release of TMS 8.0, the latest software version available for the VSX 7000 seems to be incomplete regarding management support and may be the reason for Polycom not having supportfor it in their own GMS management tool. The support for the VSX 7000 is therefore also limited in TMS(pleasee refer to the overview). Polycom is expected to bring out software updates that will allow proper management of the VSX 7000. This will in that case enable TMS to work with this type of system in the same way asit does with the Viewstation series.

The VSX 7000 does NOT have SNMP support, and will therefore NOT be autodetected on the network. Adding it to TMS therefore needs to be done manually by selecting 'Add system without SNMP support'.

Polycom ViaVideo I and II

Supported versions

Level of support related to release 5.0 of the Polycom ViaVideo Software.

Overview

Basic Monitoring

Auto Detection, Status ('No Response' or 'Alive'):	Yes
Access to internal web, ftp or telnet (if available):	Yes

Scheduling

Dial Out	No
Dial in	Yes

Advanced Monitoring

Call Status:	Yes
Call Logs:	Yes
Graphical Call Monitoring:	Yes

System Management

Upgrade	No
Templates	N/A
Settings Backup	No
Phone Book	No
Intelligent Diagnostics	Yes
Network Monitoring	Limited
View System Settings	Software Version, Gatekeeper settings, Maximum IP Bandwidth, Uptime, Call info, Management URLs
Change System Settings	None

N/A - Not Applicable

Setup

To have TMS monitor the ViaVideo, the GMS URL must be set up correctly with the location of the TMS server. Unfortunately it appears not to be possible to set this up from the user interface. To set it up manually, follow these steps:

1. Shut down the ViaVideo Application

2. Locate the file "ManagementDB.xml" on the PC the where the ViaVideo is installed. The file is typically located in folder "C:\Documents and Settings\USER_LOGIN\Application Data\Polycom\ViaVideo\ProgramSettingsXML\"

3. Open the file in a text editor, like notepad.exe

4. Search for the text "GMS_URL0"

5. 4 lines under that line there is a line containing a text similar to "<Value>sometext</Value>"

6. Edit this line so it reads "<Value>IPADDRESS_OF_TMS_SERVER/pwx/vv_status.asp</Value>" – e.g. "<Value>127.0.0.1/pwx/vv_status.asp</Value>"

7. Save and close file

8. Start the ViaVideo Application

9. Open Setup, select "Web/GMS" and verify that the newly added entry appears in the list of Global Manager URLs.

Limitations

Limited statistics reports.

Polycom iPower 600- and 900- Series

Supported versions

Level of support related to release 5.0 of the Polycom iPower series.

Overview

Basic Monitoring

Auto Detection, Status ('No Response' or 'Alive'):   Yes
Access to internal web, ftp or telnet (if available):   Yes

Scheduling

Dial Out   Yes
Dial in   Yes

Advanced Monitoring

Call Status: Yes
Call Logs: No
Graphical Call Monitoring: Yes

System Management

Upgrade   No
Templates   No
Settings Backup   No
Phone Book   No
Intelligent Diagnostics   Yes
Network Monitoring   Yes
View System Settings   Software Version, GK address, GK Mode, ISDN No,
                                                        E164 Alias, Contact info, Location info, Access Code
                                                        required, Max IP and ISDN Bandwidth, Autoanswer
                                                        mode

Change System Settings   None

Setup

In order for TMS to support the Polycom iPower, the GlobalManagement on the iPower must be enabled. This can be done from the web page of the system (webRemote -> AdminTools -> Utilities -> Global Management System -> Allow Management via Global Management System). Remember to press 'Apply changes' when done.

SNMP Community Name must be set to one of the Community Names known by TMS.
See Administrative Tools – TMS Configuration - System Interfaces - SNMP Community Name. Other required settings will be discovered by Intelligent Diagnostics when adding system to TMS.

Polycom have also documented bugs with configuring the SNMP services correctly on the iPower. This may be configured manually with higher success-rate. Take the following steps if you are unable to configure the iPower to send SNMP Traps to TMS:

1.   Log on to the iPower as Administrator user
2.   Locate the file "snmpd" (no file extension)
3.   Open file with a text editor, e.g. notepad.exe
4.   Search for text "snmpTargetAddrEntry"
5.   The last two lines in the snmpTargetAddrEntry-block should read :

   "snmpTargetAddrEntry 32 snmpUDPDomain TMS_IPADDR:0 100 3 a32 v2cExampleParams\
   nonVolatile 255.255.255.255:0 2048"

   where TMS_IPADDR is the ip-address of the TMS Server, e.g.:

   "snmpTargetAddrEntry 32 snmpUDPDomain 127.0.0.1:0 100 3 a32 v2cExampleParams\nonVolatile
   255.255.255.255:0 2048"

6.   Save file and restart the iPower.

Limitations/Notes

The Polycom iPower reports wrong bandwidths on the IP call status.

   320 kbps is reported as 256 kbps
   284 kbps is reported as 256 kbps
   512 kbps is reported as 320 kbps.

The Polycom iPower does not report the direction of calls on SNMP.

When upgrading an iPower version 4 to version 5, SNMP stops working. This is due to an error in the upgrade procedure from Polycom. Please follow the steps noted in setup to fix this error.

Sending Disconnect ALL trap to iPower always gives an error making it impossible to know whether the 'disconnect' was successful or not (although it usually DOES release the meeting). TMS therefore always assumes that the disconnect ALL (release meeting) works.

Sony PCS-1600 and PCS-6000

Supported versions

Level of support related to all versions of the Sony PCS-series.

Overview

Basic Monitoring
Auto Detection, Status ('No Response' or 'Alive'):   Yes
Access to internal web, ftp or telnet (if available):   Yes

Scheduling
Dial Out   No
Dial in   Yes

Advanced Monitoring

Call Status: No
Call Logs: No
Graphical Call Monitoring: No

System Management

Upgrade   No
Templates   No
Settings Backup   No
Phone Book   No
Intelligent Diagnostics   Yes
Network Monitoring   No
View System Settings   Limited
Change System Settings   None
N/A - Not Applicable

Setup

SNMP Community Name must be set to one of the Community Names known by TMS.
See Administrative Tools – TMS Configuration - System Interfaces - SNMP Community Name. Other required settings will be discovered by Intelligent Diagnostics when adding system to TMS.

Limitations

VTEL Galaxy

Supported versions

Level of support related to all versions of the VTEL Galaxy.

Overview

Basic Monitoring

Auto Detection, Status ('No Response' or 'Alive'):	Yes
Access to internal web, ftp or telnet (if available):	Yes

Scheduling

Dial Out	No
Dial in	Yes

Advanced Monitoring

Call Status:	No
Call Logs:	No
Graphical Call Monitoring:	No

System Management

Upgrade	No
Templates	No
Settings Backup	No
Phone Book	No
Intelligent Diagnostics	Yes
Network Monitoring	No
View System Settings	Limited
Change System Settings	None

Setup

SNMP Community Name must be set to one of the Community Names known by TMS.
See Administrative Tools – TMS Configuration - System Interfaces - SNMP Community Name. Other required settings will be discovered by Intelligent Diagnostics when adding system to TMS. The Smartnet video manager client must be installed(see vtel docs for details) to set up the VTEL Galaxy.

Limitations

Aethra Vega Star Gold

Supported versions

Level of support related to all versions of the Aethra Vega Star Gold

Overview

Basic Monitoring
Auto Detection, Status ('No Response' or 'Alive'):   Yes
Access to internal web, ftp or telnet (if available):   Yes

Scheduling
Dial Out   No
Dial in   Yes

Advanced Monitoring

Call Status: No
Call Logs: No
Graphical Call Monitoring: No

System Management

Upgrade   No
Templates   No
Settings Backup   No
Phone Book   No
Intelligent Diagnostics   Yes
Network Monitoring   No
View System Settings   Limited
Change System Settings   None

Setup

SNMP Community Name must be set to one of the Community Names known by TMS.
See Administrative Tools – TMS Configuration - System Interfaces - SNMP Community Name. Other required settings will be discovered by Intelligent Diagnostics when adding system to TMS.

Limitations

VCON

Supported versions

Level of support related to all versions of the VCON.

Overview

Basic Monitoring

Auto Detection, Status ('No Response' or 'Alive'):   Yes
Access to internal web, ftp or telnet (if available):   Yes

Scheduling

Dial Out   No
Dial in   Yes

Advanced Monitoring

Call Status: No
Call Logs: No
Graphical Call Monitoring: No

System Management

Upgrade   No
Templates   N/A
Settings Backup   No
Phone Book   No
Intelligent Diagnostics   Yes
Network Monitoring   No
View System Settings   Limited
Change System Settings   None
N/A - Not Applicable

Setup

SNMP Community Name must be set to one of the Community Names known by TMS.
See Administrative Tools – TMS Configuration - System Interfaces - SNMP Community Name. Other required settings will be discovered by Intelligent Diagnostics when adding system to TMS.

Limitations

Accord MGC

Supported versions

Level of support related to versions 5.01.82 - verified on MGC50 and MGC 100.

Overview

Basic Monitoring
Auto Detection, Status ('No Response' or 'Alive'):   Yes
Access to internal web, ftp or telnet (if available):   Yes

Scheduling
Dial Out   Yes
Dial in   Yes*

Advanced Monitoring

Call Status: Yes
Call Logs: No
Graphical Call Monitoring: No

System Management

Upgrade   No
Templates   N/A
Settings Backup   No
Phone Book   No
Intelligent Diagnostics   Yes
Network Monitoring   No
View System Settings   Limited
Change System Settings   None
N/A - Not Applicable

Setup of the Accord MGC MCU to work with TMS

SNMP Community Name must be set to one of the Community Names known by TMS.
See Administrative Tools – TMS Configuration - System Interfaces - SNMP Community Name. Other required settings will be discovered by Intelligent Diagnostics when adding system to TMS.

* - Requires Polycom Virtual Conference Suite installed on MCU

For TMS to support scheduling of incoming calls, Polycom Virtual Conference Suite is required on the MCU. Please contact your local MCU dealer for information about this suite.

To allow incoming IP-calls, please configure the H323 Network service Accordingly:
Set Gatekeeper settings, Service Mode to 'Register as Gateway' and add a E164Alias in the Prefix field, e.g. 9876. The alias must be registered under 'Span' as an Alias Name.

To use ISDN Dial-in, you must define an ISDN service on the Polycom MGC with the following name: PRI1. This service must have the dial-in numbers being used for conference dial-ins specified within the service (under the 'Spans and Phones'-tab in the service properties)
If this is not done, TMS will create dial-in numbers, but they will not be usable.

Setting up TMS to work with the Accord MGC MCU

Before being able to use the Accord MCU with TMS there are a number of steps that are needed to be taken. Because the Accord MGC does not support interrogation, many of the configurations of MCU need to be added manually in TMS. This is done by, after adding the MCU to TMS, going to its 'Other System Settings' page in System Navigator.

Virtual Conference Suite Installed

If you have VCS installed, please set this value to Yes, if not, set it to No. Without VCS you will not be able to add Dial-In calls to a conference running on the Accord MCU.

Maximum number of simultaneous conferences

Based on the configuration of the MCU, set the number of simultaneous conferences allowed. Setting this value too high may cause connection errors when setting up conferences if there are not enough resources available. Recommended value is 3.

Maximum number of simultaneous Calls

Based on the configuration of the MCU, set the number of simultaneous calls allowed regardless of which conference the call is connected to. Setting this value too high may cause connection errors when setting up calls if there are not enough resources available. Recommended value is 12 calls per videocard installed on MCU. Note that this figure is usually set lower than Maximum number of simultaneous IP + Maximum number of simultaneous ISDN Calls.

Maximum number of simultaneous IP

Based on the configuration of the MCU, set the number of simultaneous IP calls allowed regardless of which conference the call is connected to. Setting this value too high may cause connection errors when setting up calls if there are not enough resources available.

Maximum number of simultaneous ISDN Calls

Based on the configuration of the MCU, set the number of simultaneous ISDN calls allowed regardless of which conference the call is connected to. Setting this value too high may cause connection errors when setting up calls if there are not enough resources available.

It is difficult to give recommendations to default settings as the way the MCU is configured varies tremendously. Configurations that affect these settings are:

- Number and type of H323 Cards installed
- Number and type of ISDN Cards installed
- Number and type of AUDIO Cards installed
- Number and type of VIDEO Cards installed
- Number and type of MUX Cards installed
- Configuration of MUX Card per processor (number of sites x bandwidth)
- Types of calls (Mixed ISDN/IP, transcoding etc)

    We recommend beginning with safe values, running with these settings for a while and, if no resource errors occur, increase the values and continue running. If resource errors should occur, read the error descriptions and take action according to them.

After setting these values, please go to the System Information page and press the 'Force Refresh button before continuing with the configuration!

Setting up ISDN Base Numbers and E164 Aliases

After pressing update on the 'Other System Settings' page, please go to the 'Intelligent Diagnostics' page.

Depending on the Maximum number of simultaneous calls set on the previous page, you will now find an input field per conference for adding an E164 alias. The MCU is typically only set up with one E164 Alias. Please enter this Alias in all the E164Alias-fields and postfix it with the conference number. E.g: if MCU E164 alias is set to 9876 and you have specified max 4 simultaneous conferences you will have to fill out the fields like this:

E164 Alias 1: 9876*1*
E164 Alias 2: 9876*2*
E164 Alias 3: 9876**3**
E164 Alias 4: 9876**4**
It is very important that the postfix number reflects the conference number!

Depending on the Maximum number of simultaneous calls set on the previous page, you will now find an input field per conference for adding an ISDN Base Number. The MCU is typically set up with a number range. Please enter one unique ISDN Number from this range per conference. E.g: if MCU Number Range is set to 2121230000-2121230011 and you have specified max 4 simultaneous conferences you can fill out the fields like this:

ISDN base number: 2121230000
ISDN base number: 2121230002
ISDN base number: 2121230001
ISDN base number: 2121230009

The number range set on the MCU can be found by using the Polycom MGC Manager. Log on to the MCU, select Network Services, ISDN and on the service (e.g. named PRI1) , right click and select Properties. Select the TAB called 'Spans and Phones' and look under the section 'Dial In Phone Num' for valid ISDN Numbers. If you enter a number in TMS which does not exist in this span you will get a 'PHONE_NO_SUCH_NUMBER' error when trying to create a conference.

Setting up Gatekeeper Settings

On the Intelligent Diagnostics page, please set the Gatekeeper Mode to 'Manual' and enter the gatekeeper ip-address the MCU is registered to in Requested Gatekeeper address field. When updating settings the Registered Gatekeeper address field will also be updated with this ip-address.

Limitations

Cisco and RadVision MCU ViaIP15-100

Supported versions

Level of support related to the following releases from Cisco and RadVision:

1. RADVISION ViaIP MCU 15, version 2.2.65 and newer
2. RADVISION ViaIP MCU 30, version 2.2.65 and newer
3. RADVISION ViaIP MCU 60, version 2.2.65 and newer
4. RADVISION ViaIP MCU 100, version 2.2.65 and newer
5. CISCO IPVC-3540-MCU, version 2.2.65 and newer
6. CISCO IPVC-3511-MCU, version 2.2.65 and newer

Overview

Basic Monitoring

Auto Detection, Status ('No Response' or 'Alive'):	Yes
Access to internal web, ftp or telnet (if available):	Yes

Scheduling

Dial Out	Yes
Dial in	Yes

Advanced Monitoring

Call Status:	Yes
Call Logs:	No
Graphical Call Monitoring:	No

System Management

Upgrade	No
Templates	No
Settings Backup	No
Phone Book	N/A
Intelligent Diagnostics	Yes
Network Monitoring	Yes
View System Settings	Limited
Change System Settings	None

N/A - Not Applicable

Setup

How to configure the Cisco and Radvision MCU

The following steps are needed in order to manage conferences on the Cisco and Radvision MCU's in TMS 8.0

The MCU resources managed by TMS need to have a specific service prefix description to allow TMS to recognize the reserved resource. The TMS Conference Services are added to the Services list using the web interface on the MCU.

The following steps describe how to add TMS Conference Services description on the MCU:

1   Enter the Web interface on the MCU and select the Services page. Add a new Service pressing the Add-button, or edit one of the existing Services.

Figure 1: MCU Web page, Configuring Services (MCU->Services)

2.   Click the Add or Edit-button to open the Add or Edit service page.

3.   Enter a unique H323 Prefix number for this Service (see 'Suggested number planning' at the end of this document on selecting unique prefixes).

4.   Set the Description field to be: "**TMS Conference"**. This is a unique identifier used by TMS to identify that this Service has been reserved for TMS Scheduling. This field is case sensitive. You do not need to enter any other information, as this will be configured automatically by TMS.

Figure 2: MCU Web page, Edit Services (MCU->Services->Add/Edit)

5.   You must define 1 service prefix for each simultaneous conference you would like to create on this MCU. Repeat steps 1– 4 for the number of Services (simultaneous Conferences) you wish to manage for this MCU through TMS. Each Service must use a **different** Service Prefix but all must have the **same** description "TMS Conference".
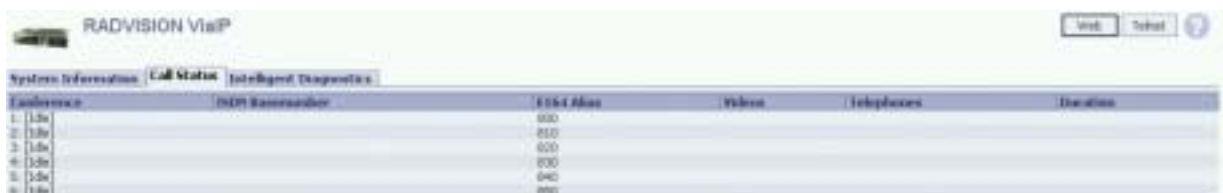
Restrictions on TMS Conference Services

TANDBERG Suggests that all conferences on a MCU managed by TMS be initiated only by TMS. This is due to the following restrictions:

1.   If a Service reserved by TMS (TMS Conference) is used without Scheduling the conference from TMS, then TMS will disconnect that conference automatically when TMS needs to use this conference.

2.   TMS calculates the available resources needed for a call, and reserves this on the MCU.

3.   An ad-hoc MCU conference not initiated by TMS will use resources that TMS is unaware of and cause the TMS Conference allocation to fail.

4.   Removing all non-TMS services from the MCU service list can help limit the possibility of ad-hoc calls interfering with TMS Scheduling.

Verify correct MCU Services

1.   Start TMS and add your MCU to TMS (see user manual)

2.   Select System Management -> Navigator -> your MCU. Click on your MCU and select the "Call Status" tab

3.   To verify that all the Services you configured on the MCU are recognized correctly, the number of Services configured should be the same as number of Conferences shown on this page.

Figure 3: TMS Web Page, Navigator (MCU->System Status

4   The Services you reserved as "TMS Conferences" are shown with status "Idle". When a Service (or conference) has been Scheduled by TMS, it will show up as "TMS ConferenceN", were N is a number from 1 to the number of conferences allocated. As seen with in the MCU Web page:
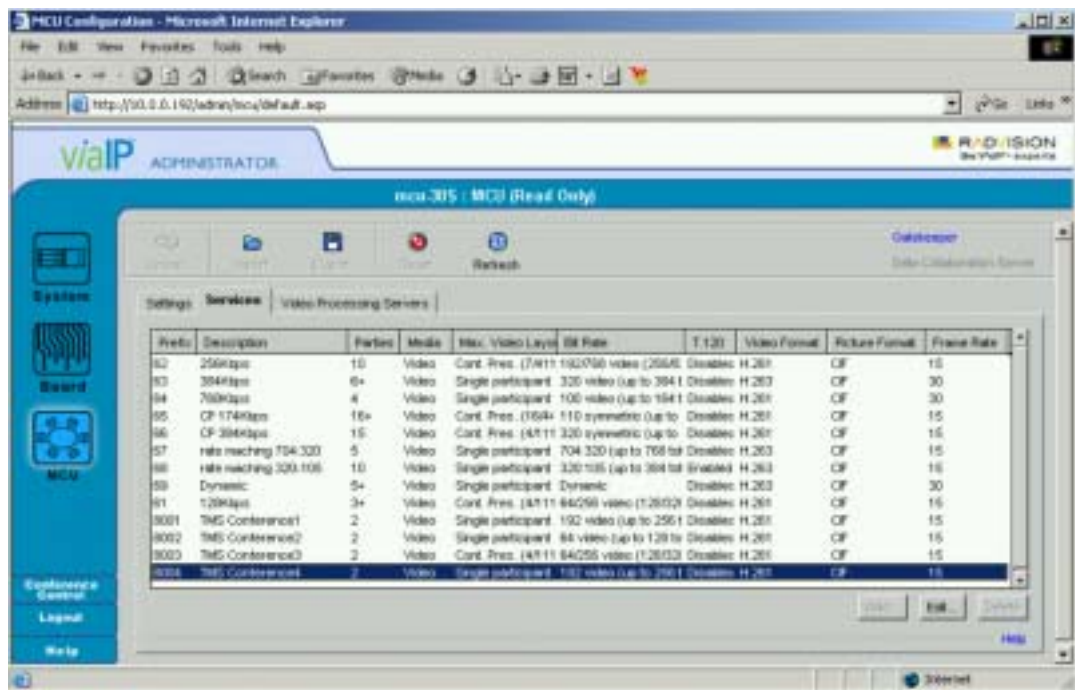
Figure 4: MCU Web page, Showing TMS Conferences

Suggested number planning

As conferences in your H323 network needs to have unique conference ID's. As the service prefix on the MCU is used to generate the unique conference ID, the service prefix also needs to be unique on the H323 network. To accomplish this, TANDBERG have following guidelines for selecting service prefixes:

1.   Let the first two digits of the service prefix uniquely identify the MCU in the H323 network. Try not to start the service prefix with "0" or "1" as these numbers often are reserved in the H323 network.

2.   Let the succeeding two digits uniquely identify the service on the MCU.

E.g.:   Service prefix 8101 represents the first service on the first MCU.
        Service prefix 8202 represents the second service on the first MCU.
        Service prefix 8203 represents the third service on the second MCU.

Participants on the Radvision MCU's

Bit-rate	Video Mode	MCU15	MCU30	MCU60	MCU100
64kbs	VS	26	45	90	150
128kbs	VS	17	30	60	100
128kbs	CP	17	30	60	100
192kbs	VS	11	19	38	64
192kbs	CP	11	19	38	64
256kbs	VS	10	18	35	59
256kbs	CP	10	18	35	59
320kbs	VS	10	17	34	57
320kbs	CP	10	17	34	57
384kbs	VS	9	15	30	50
384kbs	CP	9	15	30	50
512kbs	VS	9	15	30	50
768kbs	VS	6	10	21	35
1152kbs	VS	5	9	19	31
1474kbs	VS	4	8	15	25
1920kbs	VS	4	6	13	21

SNMP Community Name must be set to one of the Community Names known by TMS.
See Administrative Tools – TMS Configuration - System Interfaces - SNMP Community Name. Other required settings will be discovered by Intelligent Diagnostics when adding system to TMS.

Limitations

Cisco and RadVision Gateway

Supported versions

Level of support related to the following releases from Cisco and RadVision:

RADVISION ViaIP Gateway, version 2
Cisco Gateway, version 2

Overview

Basic Monitoring

Auto Detection, Status ('No Response' or 'Alive'):	Yes
Access to internal web, ftp or telnet (if available):	Yes

Scheduling

Dial Out	N/A
Dial in	N/A

Advanced Monitoring

Call Status:	Yes
Call Logs:	No
Graphical Call Monitoring:	N/A

System Management

Upgrade	No
Templates	No
Settings Backup	No
Phone Book	N/A
Intelligent Diagnostics	Yes
Network Monitoring	Yes
View System Settings	Limited
Change System Settings	None

N/A - Not Applicable

Setup

The following steps should be verified to make sure that TMS is able to use the gateway.

Enabling TCS4

To be able to call ISDN to IP with TMS, you should enable TCS4.

Select the first enabled Port, either 'Pri Port 1' or 'Pri Port 2', and select the Call Policies menu item. TCS4 should be enabled.

Gateway services

To call IP to ISDN, the gateway must be configured with gateway services. The following services are recommended:

1.   Video services with the bit rate set to 'Auto' and call type set to 'Video'.

2.   Telephone service with call type set to 'Voice'.

Figure 5: A sample showing a configured voice service and a video service with bit rate set to 'Auto'

The voice service prefix and the video service prefix can be entered into the gateway configuration of a location in TMS.

Gatekeeper address

The gateway services are available to the endpoints registered on the same gatekeeper as the gateway. The gateway should be registered at the same gatekeeper as the endpoints using the gateway services.

SNMP Traps

The RadVision Gateway can send out SNMP traps. To configure SNMP traps, se the Settings -> Alert Indications tab in the admin GUI. The SNMP traps IP-address should be set to the IP-address of the TMS-server.

Figure 6: The SNMP traps configuration page.

Limitations

Limited statistics

Cisco IOS Gatekeeper

Supported versions

Supported Cisco Software: Version 12.1(5) <u>or</u> Version 12.2(13) T.

Overview

Basic Monitoring

Auto Detection, Status ('No Response' or 'Alive'):	Yes
Access to internal web, ftp or telnet (if available):	Yes

Scheduling

Dial Out	N/A
Dial in	N/A

Advanced Monitoring

Call Status:	Yes
Call Logs:	N/A
Graphical Call Monitoring:	N/A

System Management

Upgrade	No
Templates	No
Settings Backup	Yes
Phone Book	N/A
Intelligent Diagnostics	Yes
Network Monitoring	Yes
View System Settings	Limited
Change System Settings	None

N/A - Not Applicable

Setup

In order to be supported by TMS, Cisco IOS Gatekeepers require

> A Read/Write SNMP community name
> The standard telnet password
> The administrator level password

Setting a Read/Write SNMP community name

The SNMP community name is used by the TMS discovery protocol to determine if a system exists or not. Therefore it is vital that the Cisco Gatekeeper has an SNMP community name.

The steps to ensure this are:

1.   Open a telnet session to the Cisco gatekeeper on port 23
2.   Type in the standard telnet password and press enter
3.   Type "enable" and press enter
4.   Type in the administrator password and press enter
5.   Type "configure terminal" and press enter
6.   Type "snmp-server community private rw" and press enter
7.   Type "end" and press enter
8.   Type "exit" and press enter

Note: *That in the above example the community name is "private" this is the standard, but it is possible to set it to anything else.*

Interzone Calls:

In order for TMS to create a conference route between two gatekeepers in different zones, both gatekeepers MUST have a local zone prefix. The gatekeeper in the other zone must be registered as a neighbour (remote zone) and must have the correct zone prefix.

To register the local zone:

1.   Open a telnet session to the Cisco gatekeeper on port 23
2.   Type in the standard telnet password and press enter
3.   Type "enable" and press enter
4.   Type in the administrator password and press enter
5.   Type "configure terminal" and press enter
6.   Type "gatekeeper" and press enter
7.   Type "zone local <name of gatekeeper> <domain> <IP address>" and press enter
8.   Type "end" and press enter
9.   Type "exit" and press enter

e.g. zone local gk-cisco1 TANDBERG 10.0.0.1

To register a neighbour (remote zone):

1. Open a telnet session to the Cisco gatekeeper on port 23
2. Type in the standard telnet password and press enter
3. Type "enable" and press enter
4. Type in the administrator password and press enter
5. Type "configure terminal" and press enter
6. Type "gatekeeper" and press enter
7. Type "zone remote <name of gatekeeper> <domain> <IP address>" and press enter
8. Type "end" and press enter
9. Type "exit" and press enter

e.g. zone remote gk-cisco2 TANDBERG 10.0.0.2
    zone remote gk-radvision1 TANDBERG 10.0.0.3

Creating zone prefixes:

1. Open a telnet session to the Cisco gatekeeper on port 23
2. Type in the standard telnet password and press enter
3. Type "enable" and press enter
4. Type in the administrator password and press enter
5. Type "configure terminal" and press enter
6. Type "gatekeeper" and press enter
7. Type "zone prefix <name of gatekeeper> <domain> <prefix>" and press enter
8. Type "end" and press enter
9. Type "exit" and press enter

e.g. zone prefix gk-cisco1 212
    zone prefix gk-radvision1 713
    zone prefix gk-cisco2 619

Limitations

Limited Statistics

TMS Backup & Restore

When backup or restore of system settings is performed from TMS, ONLY SNMP and Gatekeeper settings are saved under Backup and ONLY SNMP and Gatekeeper settings are restored under Restore. No other settings (such as ip / password /network interfaces etc…) will be saved.

Radvision Gatekeeper ViaIP

Supported versions

Supported software version: RADVISION ViaIP Gatekeeper, version 3

Overview

Basic Monitoring
Auto Detection, Status ('No Response' or 'Alive'):   Yes
Access to internal web, ftp or telnet (if available):   Yes

Scheduling
Dial Out   N/A
Dial in   N/A

Advanced Monitoring

Call Status: Yes
Call Logs: No
Graphical Call Monitoring: N/A

System Management

Upgrade   No
Templates   No
Settings Backup   No
Phone Book   N/A
Intelligent Diagnostics   Yes
Network Monitoring   Yes
View System Settings   Limited
Change System Settings   None

N/A - Not Applicable

Setup

The support for this gatekeeper includes:

1. Viewing selected settings
2. Viewing registered endpoints
3. Viewing available services
4. Viewing active calls
5. Verifying that a endpoints is registered on a gatekeeper
6. Intelligent diagnostics

The menus are described in the text below with the following notation (Settings -> Calls), meaning the Settings tab, and selecting the Calls menu. All menu operations are located through the admin console of the gatekeeper: http://<ip-address to the gatekeeper>/admin/
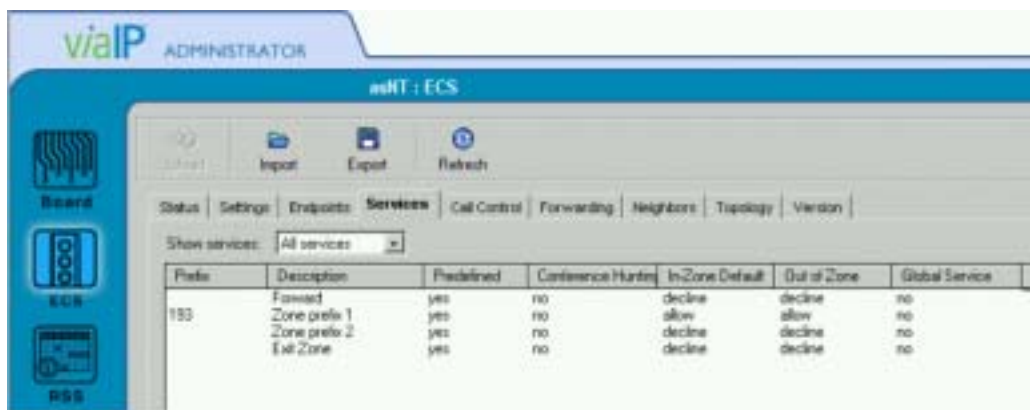
The following steps should be verified to make sure that TMS is able to use the gatekeeper.

The following settings should be verified:

1.   Enable 'Accept Calls' (Settings -> Calls)

Neighbouring zone prefix

On a Radvision Gatekeeper you do not have to use a prefix to call endpoints on another zone. If you want zone prefixes you can set a prefix through the predefined service 'Zone Prefix 1' or 'Zone Prefix 2'. Setting zone prefix will force all calls into the gatekeeper to use the configured prefix.

Figure: An example of a Zone Prefix configured to be 193. Out Of Zone has to be allowed.

Neighbouring zones

If the videoconference network is divided into several zones, the gatekeepers from different zones should be added as neighbours.

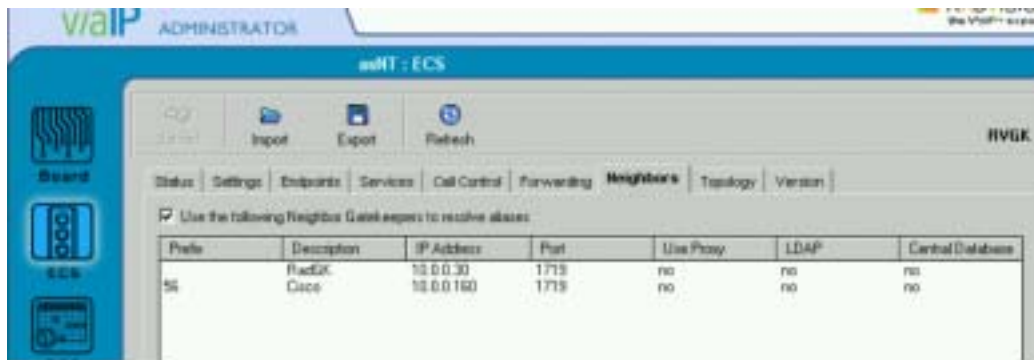Between Radvision Gatekeepers you do not need to use zone prefixes, into a Cisco gatekeepers you have to.

Figure: Configuration of neighboring zones

Endpoint registration

The Radvision Gatekeeper has three modes for endpoint registration (Settings -> Basics). The endpoints registration mode is viewed under Settings in TMS.

Everyone: The endpoints can register by using the gatekeeper IP-address.

Predefined: The endpoints must be manually entered from the Endpoints tab.

No endpoints: No endpoint is allowed to register.

Limitations

Glossary

Administrator rights

The highest level of access a user can have.

Application

Application is a term used to describe the different ways that a videoconferencing system is used. Two common applications are in the field of medicine (Telemedicine) and eduction (Distance Education).

Bandwidth

The effective carrying capacity of a telecommunications transmission medium. Bandwidth describes how much information can be pushed through an electronic "pipe" at any given time. In analog systems, it is the difference between the highest frequency that a channel can carry and the lowest, measured in hertz. In digital systems the unit of measure of bandwidth is bits per second. For instance, a voice transmission by telephone requires a bandwidth of about 3000 cycles per second (3KHz). A TV channel occupies a bandwidth of 6 million cycles per second (6 MHz) in terrestrial Systems. In videoconference based systems a larger bandwidth of 17.5 to 72 MHz is used to spread or "dither" the television signal in order to prevent interference.

Billing code

Billing codes protects access to calling out from a videoconference system.

Ethernet/LAN Connector

Ethernet/LAN Connector (10/100Mb) for integration into a Local Area Network. By integrating into the LAN, the latest software upgrades may be uploaded. Network management facilities allow MIS personnel better control over the network. Remote diagnostics can be achieved over the LAN.

Event

Happening, occurrence. Examples: A system enters a call, a systems boots etc.

FTP (File Transfer Protocol)

Allows a user to transfer files electronically from remote computers back to the user's computer. The feature is part of the TCP/IP/FTP software suite.

IIS

Internet Information Services, a web-server by Microsoft.

IP

An industry standard, connectionless, best-effort packet switching protocol used as the network layer in the TCP/IP Protocol Suite.

ISDN

Integrated Services Digital Network is an international standard for digital services on the public switched telephone network.

LAN

Local Area Network. A high volume data transmission signal is returned to the sending device after passing through all or part of a communications link or network.

Admin Password Protection

The videoconferencing system's stored network configuration set-up can be password protected. This ensures that unauthorized changes to the set-up do not occur.

PBX (Private Branch Exchange)

A telephone switch, usually located on a customer's premises, connected to the telephone network but operated by the customer. A PBX provides pooled access to a given number of inside (extension) lines in a smaller number of outside lines (trunks). Often, outgoing calls are dialled directly; incoming calls are handled by an operator or switched automatically by the PBX software.

Remote Software Upgrades

Remote software upgrade means that software can be uploaded to the videoconferencing system through LAN or ISDN using a standard serial port, File Transfer Protocol (FTP), or a standard web browser.

Script

A program that is not compiled but executed and translated on the fly.

Session

A connection to a web-server by a user that will time out if the user does not perform any actions within a timeframe.

Setting Template

Settings that are not unique to a system, but can be equal on a number of systems is combined to a settings template.

Site

A geographic location where there is at least one person that wants to have a meeting with at least one other person at another geographic location

SNMP

SNMP is a built-in protocol allowing simple network management. Supports TANDBERG SNMP version 2 (with mib-2 (RFC1213)) for network monitoring through LAN interface. This is ideal for large companies with extensive IT networks because SNMP can be easily integrated into existing LAN/WAN network monitoring environments using standard tools and applications.

Streaming

The streaming function lets you broadcast video and audio to PCs linked to the Local Area Network (LAN) or over the Internet. This is an excellent tool for distributing a speech or presentation within or between organizations. The video from the streaming site can be seen at the same time as audio from both sides of a point-to-point call will be heard. Streaming is also a useful tool for better remote management.

Subnet

The subnet is used to identify the parts of an IP-Address that correspond to the different sections (separated by dots). It's also known as the "subnet mask" since the network portion of an address can be determined by the encoding inherent in an IP- address.

TANDBERG Management Suite

Allows videoconferencing systems to be monitored, managed and maintained from a central web portal.

TCP/IP (Transmission Control Protocol/Internet Protocol)

Is a combined set of protocols that performs the transfer of data between two computers. TCP monitors and ensures correct transfer of data. IP receives the data from TCP, breaks it up into packets, and ships it off to a network within the Internet. TCP/IP is also used as a name for a protocol suite that incorporates these functions and others.

TELNET

An application using the TCP/IP suite of software protocols that handles terminals. Among other functions, it allows a user to log in to a remote computer from the user's local computer.

Telnet-based Remote Network and System Diagnostics

Using Telnet, all Codec adjustments, diagnostics and fault determination can be performed remotely. This minimizes down time, and allows technical support to accurately identify system or network issues and to execute the necessary solution.

TMS

See TANDBERG Management Suite

Traps

A systems part of the SNMP protocol to inform a manager on the network about events that has happened on the unit.

WAN (Wide Area Network)

A communications network that services a geographic area larger than that served by a local area network or metropolitan area network. WANs include commercial or educational dial-up networks such as CompuServe, Internet or BITNET etc.

[1]   Microsoft Windows 2000 and Microsoft Internet Information Services are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Appendix

Access levels in TMS

The table below describes the different access levels and lists the priviliges granted to a user for a system with such access levels set. Note that a user's access level to a system is deteminded by which groups this user is a member of.

The different access levels that can be set on a system or folder is as following:

A   - Administrator (user has access to a system/folder with Admin access level)
M   - Monitor (user has access to a system with Monitor access level)
B   - Book (user has access to a system with Use access level)
NA   - No Access (user does not have access to system)

	A	M	B	NA
System Configuration and Navigation				
Can view configuration of system	Yes	Yes	Limited	
Can "Edit System Information"	Yes			
Can view current call status on a system along-with disconnecting and adding call participants.	Yes	Yes		
Can send a message to the system	Yes	Yes		
Can access systems web, telnet and ftp interfaces	Yes			
Can change access rights on a system.	Yes			
Can change access rights on folder.	Yes			
Directories				
Can update systems with a TMS directory	Yes			
Can view directory on system	Yes	Yes	Yes	

	A	M	B	NA
Access codes				
Can update systems with access codes	Yes			
Settings				
Can create setting backups	Yes			
Can restore setting backups	Yes			
Can view current settings on system and compare to stored settings	Yes	Yes		
Templates				
Can view templates	Yes			
Can update systems with templates	Yes			
Can update system wuth template	Yes			
Statistics				
Can view and export system statistics	Yes	Yes		
System Upgrade				
Can upgrade software on systems	Yes			
Monitoring				
Can subscribe to events from systems	Yes	Yes		
Advanced Booking				
Can book a meeting with system	Yes	Yes	Yes	

A user with monitor level access can view settings and configurations to check for problems, along with dialing and disconnecting participants. A user with Monitor level access does however not have access to change the settings on a system.

A user with Book level access can use the system to make calls using the scheduler.

Cause Codes

Cause No. -1 - Undefined cause code

TANDBERG specific. Not part of ITU-T Cause Code standard.

Cause No. 0 - Undefined cause code

TANDBERG specific. Not part of ITU-T Cause Code standard.

Cause No. 1 - Unallocated (Unassigned) Number

This cause indicates that the destination requested by the calling user cannot be reached because, although the number is in a valid format, it is not currently assigned.

Cause No. 2 - No Route To Specified Transit Network

This cause indicates that the equipment sending this cause has received a request to route the call through a particular transit network which it does not recognize. The equipment sending this cause does not recognize the transit network either because the transit network does not exist or because that particular transit network, while it does exist, does not serve the equipment which is sending this cause.

Cause No. 3 - No Route To Destination

This cause indicates that the called party cannot be reached because the network through which the call has been routed does not serve the destination desired. This cause is supported on a network dependent basis.

Cause No. 4 - Send Special Information Tone (Five One Zero NT)

This cause indicates that the called party cannot be reached for reasons that are of a long term nature and that the special information tone should be returned to the calling party.

Cause No. 5 - Misdialed Trunk Prefix

This cause indicates the erroneous inclusion of a trunk prefix in the called party number. This number is supposed to be stripped from the dialed number being sent to the network by the customer premises equipment.

Cause No. 6 - Channel Unacceptable

This cause indicates that the channel most recently identified is not acceptable to the sending party for use in this call.

Cause No. 7 - Call awarded, being delivered in an established channel

This cause indicates that the user has been awarded the incoming call, and that the incoming call is being connected to a channel already established to that user for similar calls (e.g. packet-mode x.25 virtual calls).

Cause No. 8 - Preemption

This cause indicates the call is being preempted.

Cause No. 9 - Preemption - Circuit Reserved For Reuse

This cause indicates that the call is being preempted and the circuit is reserved for reuse by the preempting exchange.

Cause No. 16 - Normal Call Clearing

This cause indicates that the call is being cleared because one of the users involved in the call has requested that the call be cleared.

Cause No. 16/4 or 17 - User Busy

This cause is used when the called user has indicated the inability to accept another call. This cause code may be generated by the called user or by the network. Please note that the use equipment is compatible with the call.

Cause No. 16/3 or 18 - No User Responding

This cause is used when a called party does not respond to a call establishment message with either an alerting or connect indication within the prescribed period of time allocated (in Q.931 by the expiry of either time T303 or T310).

Cause No. 19 - No Answer From User (User Alerted)

This cause is used when a user has provided an alerting indication but has not provided a connect indication within a prescribed period of time. Note: This cause is not necessarily generated by the customer premise equipment, but may be generated by internal network timers.

Cause No. 20 - Subscriber Absent

This cause value is used when a mobile station has logged off, radio contact is not obtained with a mobile station or if a personal telecommunication user is temporarily not addressable at any user-network interface.

Cause No. 21 - Call Rejected

This cause indicates that the equipment sending this cause does not wish to accept this call, although it could have accepted the call because the equipment sending this cause is neither busy nor incompatible. This cause may also be generated by the network, indicating that the call was cleared due to a supplementary service constraint. The diagnostic field may contain additional information about the supplementary service and reason for rejection.

Cause No. 22 - Number Changed

This cause is returned to a calling party when the called party number indicated by the calling party is no longer assigned. The new called party number may optionally be included in the diagnostic field. If the network does not support this cause, cause no: 1, unallocated (unassigned) will be used instead.

Cause No. 26 - Non-Selected User Clearing

This cause indicates that the user has not been awarded the incoming call.

Cause No. 27 - Destination Out Of Order

This cause indicates that the destination cannot be reached because the interface to the destination is not functioning correctly. The signaling message was unable to be delivered due to a hardware failure.

Cause No. 28 - Invalid Number Format (Address Incomplete)

This cause indicates that the called party cannot be reached because the called party number is not in a valid format or is not complete.

Cause No. 29 - Facilities Rejected

This cause is returned when a facility requested by the user cannot be provide by the network.

Cause No. 30 - Response To Status Inquiry

This cause is included in the STATUS message when the reason for generating the STATUS message was the prior receipt of a STATUS ENQUIRY.

Cause No. 31 - Normal, Unspecified

This cause is used to report a normal event only when no other cause in the normal class applies.

Cause No. 34 - No Circuit/Channel Available

This cause indicates that there is no appropriate circuit/channel presently available to handle the call. Note: If you receive this call, try another data-service, such as dropping from a 64K to 56K data rate.

Cause No. 35 - Call Queued

This cause indicates that the call has been queued for service by the next available device.

Cause No. 38 - Network Out Of Order

This cause indicates that the network is not functioning correctly and that the conditions are likely to last a relatively long period of time. A call that is attempted soon afterwards will most likely not connect successfully.

Cause No. 39 - Permanent Frame Mode Connection Out-Of-Service

This cause is included in a STATUS message to indicate that a permanently established frame mode connection is out-of-service (e.g. due to equipment or section failure) [see Annex A/Q.933]

Cause No. 40 - Permanent Frame Mode Connection Operational

This cause is included in a STATUS message to indicate that a permanently established frame mode connection is operational and capable of carrying user information. [see Annex A/Q.933]

Cause No. 41 - Temporary Failure

This cause indicates that the network is not functioning correctly and that the condition is not likely to last a very long period of time. A call that is attempted almost immediately afterwards will most likely connect successfully.

Cause No. 42 - Switching Equipment Congestion

This cause indicates that the switching equipment generating this cause is experiencing a period of high traffic.

Cause No. 43 - Access Information Discarded

This cause indicates that the network could not deliver access information, low layer compatibility, high layer compatibility, or sub-address as indicated in the diagnostic.

Cause No. 44 - Requested Circuit/Channel Not Available

This cause is returned when the circuit or channel indicated by the requesting entity cannot be provided by the other side of the interface.

Cause No. 46 - Precedence Call Blocked

This cause indicates that there are no preemptable circuits or that the called user is busy with a call of equal or higher preemptable level.

Cause No. 47 - Resource Unavailable, Unspecified

This cause is used to report a resource unavailable event only when no other cause in the resource unavailable class applies.

Cause No. 49 - Quality Of Service Not Available

This cause is used to report that the requested Quality of Service cannot be provided (delay canít be supported).

Cause No. 50 - requested facility not subscribed

This cause indicates that the requested supplementary service could not be provided due to user oversight. This cause code is often caused by the CPE being configured for the wrong switch type.

Cause No. 52 - outgoing calls barred

This cause indicates that because of call screening provided by the network, the calling user is not permitted to make a call.

Cause No. 53 - Outgoing Calls Barred Within CUG

This cause indicates that although the calling party is a member of the CUG for the outgoing CUG call, outgoing calls are not allowed for this member of the CUG.

Cause No. 54 - incoming calls barred

This cause indicates that the called user will not accept the call delivered in the SETUP message.

Cause No. 55 - Incoming Calls Barred Within CUG

This cause indicates that although the calling party is a member of the CUG for the incoming CUG call, incoming calls are not allowed for this member of the CUG.

Cause No. 57 - Bearer Capability Not Authorized

This cause indicates that the user has requested a bearer capability which is implemented by their equipment but the user is not authorized to use.

Cause No. 58 - Bearer Capability Not Presently Available

This cause indicates that the user has requested a bearer capability which is implemented by the equipment which generated this cause but which is not available at this time.

Cause No. 62 - Inconsistency In Outgoing Information Element

This cause indicates an inconsistency in the designated outgoing access information and subscriber class.

Cause No. 63 - Service Or Option Not Available, Unspecified

This cause is used to report a service or option not available event only when no other cause in the service or option not available class applies.

Cause No. 65 - Bearer Capability Not Implemented

This cause indicates that the equipment sending this cause does not support the bearer capability requested.

Cause No. 66 - Channel Type Not Implemented

This cause indicates that the equipment sending this cause does not support the channel type requested.

Cause No. 69 - Requested Facility Not Implemented

This cause indicates that the equipment sending this cause does not support the requested supplemental service.

Cause No. 70 - Only Restricted Digital Information Bearer Capability Is Available

This cause indicates that on equipment has requested an unrestricted bearer service but that the equipment sending the cause only supports the restricted version of the requested bearer capability.

Cause No. 79 - Service Or Option Not Implemented, Unspecified

This cause is used to report a service r option not implemented but only when no other cause in this class applies.

Cause No. 81 - Invalid Call Reference Value

This cause indicates that the equipment sending this cause has received a message with a call reference which is not currently in use on the user-network interface.

Cause No. 82 - Identified Channel Does Not Exist

This cause indicates that the equipment sending this cause has received a request to use a channel not activated on the interface for a call. For example, if the user only subscribed to channels 1 to 12 and channel 13 through 23 is requested by either side, this cause is generated.

Cause No. 83 - A Suspended Call Exists, But This Call Identify Does Not

This cause indicates that a call resume has been attempted with a call identity which differs from that in use for any presently suspended call(s).

Cause No. 84 - Call Identity In Use

This cause indicates that the network has received a call resume request. The call resume request contained a call identity information element which presently does not indicate any suspended call within the domain of interfaces over which calls may be resumed.

Cause No. 85 - No Call Suspended

This cause indicates that the network has received a call resume request containing a Call identity information element which presently does not indicate any suspended call within the domain of interfaces over which calls may be resumed.

Cause No. 86 - Call Having The Requested Call Identity Has Been Cleared

This cause indicates that the network has received a call resume request. The request contained a call identity information element which once indicated a suspended call, however, that the call was cleared while suspended (either a network time-out or remote user).

Cause No. 87 - User Not A Member Of CUG

This cause indicates that the called user for the incoming CUG call is not a member of the specified CUG or that the calling user is an ordinary subscriber calling a CUG subscriber.

Cause No. 88 - Incompatible Destination

This cause indicates that the equipment sending this cause has received a request to establish a call which has low layer compatibility, high layer compatibility, or other compatibility attributes (e.g. data rate) which cannot be accommodated.

Cause No. 90 - Non-Existent CUG

This cause indicates that the specified CUG does not exist.

Cause No. 91 - Invalid Transit Network Selection

This cause indicates that a transit network identification was received which is of an incorrect format as defined in Annex C/Q.931

Cause No. 95 - Invalid Message, Unspecified

This cause is used to report an invalid message event only when no other cause in the invalid class applies.

Cause No. 96 - Mandatory Information Element Is Missing

This cause indicates that the equipment sending this cause has received a message which is missing an information element which must be present in the message before that message can be processed.

Cause No. 97 - Message Type Non-Existent Or Not Implemented

This cause indicates that the equipment sending this cause has received a message with a message type it does not recognize either because this is a message not defined of defined but not implemented by the equipment sending this cause.

Cause No. 98 - Message Not Compatible With Call State Or Message Type Non-Existent Or Not Implemented

This cause indicates that the equipment sending this cause has received a message such that the procedures do not indicate that this is a permissible message to receive while in the call state, or a STATUS message was received indicating an incompatible call state.

Cause No. 99 - Information Element / Parameter Non-Existent Or Not Implemented

This cause indicates that the equipment sending this cause has received a message which includes information element(s)/parameter(s) not recognized because the information element(s)/parameter name(s) are not defined or are defined but not implemented by the equipment sending the cause. This cause indicates that the information element(s)/parameter(s) were discarded. However, the information element is not required to be present in the message in order for the equipment sending the cause to process the message.

Cause No. 100 - Invalid Information Element Contents

This cause indicates that the equipment sending this cause has received and information element which it has implemented; however, one or more fields in the information elements are coded in such a way which has not been implemented by the equipment sending this cause.

Cause No. 101 - Message Not Compatible With Call State

This cause indicates that a message has been received which is incompatible with the call state.

Cause No. 102 - Recovery On Timer Expiry

This cause indicates that a procedure has been initiated by the expiry of a timer in association with Q.931 error handling procedures.

Cause No. 103 - Parameter Non-Existent Or Not Implemented - Passed On

This cause indicates that the equipment sending this cause has received a message which includes parameters not recognized because the parameters are not defined or are defined but not implemented by the equipment sending this cause.

Cause No. 110 - Message With Unrecognized Parameter Discarded

This cause indicates that the equipment sending this cause has discarded a received message which includes a parameter that is not recognized.

Cause No. 111 - Protocol Error, Unspecified

This cause is used to report a protocol error event only when no other cause in the protocol error class applies.

Cause No. 127 - Interworking, Unspecified

This cause indicates that there has been internetworking which does not provide causes for actions. The precise cause for a message being sent is not known.

Cause No. 128 - Remote Is Busy

TANDBERG specific. Not part of ITU-T Cause Code standard.

Cause No. 129 - Call rejected by remote

TANDBERG specific. Not part of ITU-T Cause Code standard.

Cause No. 130 - Destination unrechable

TANDBERG specific. Not part of ITU-T Cause Code standard.

Cause No. 131 - Unknown reason

TANDBERG specific. Not part of ITU-T Cause Code standard.

Cause No. 132 - Generic error

TANDBERG specific. Not part of ITU-T Cause Code standard.

Cause No. 133 - Gatekeeper rejected call

TANDBERG specific. Not part of ITU-T Cause Code standard.

Cause No. 134 - Gatekeeper could not find number

TANDBERG specific. Not part of ITU-T Cause Code standard.

Cause No. 135 - Gatekeeper timed out call

TANDBERG specific. Not part of ITU-T Cause Code standard.

Cause No. 136 - Gatekeeper not active

TANDBERG specific. Not part of ITU-T Cause Code standard.

Cause No. 255 - Undefined cause code

TANDBERG specific. Not part of ITU-T Cause Code standard.

Index