TANDBERG Management Suite 11.7 Administrator's guide

TANDBERG

D13741, Rev 5

Table of Contents

1 Introduction

This document is meant to describe in detail the conceptual parts of TANDBERG Management Suite (TMS) that are not covered in the *TMS Help Texts*.

For information about the level of support for the different devices in TMS please refer to the *3rd Party Support Document*.

For information about configuration of the different booking APIs (Microsoft Exchange, Lotus Domino and the 3rd Party Booking API) please refer to the appropriate documentation found on the TMS CD.

TMS 11 requires SQL/MSDE 2000 or newer. Information on how to upgrade the database server is found in the *database upgrade document* on the TMS CD.

For information on how to install TANDBERG See&Share please refer to the *See&Share Admin Guide* found on the TMS CD, and for information on how to use it please refer to the *See&Share User Guide* that is also on the CD.

2 Zones

The point of having Zones is to enable TMS to dial the correct numbers when dialing on ISDN between countries and area codes within the same country, picking which systems should use IP and which should use ISDN between them, and insert the correct prefixes for IP systems when using an ISDN gateway.

Systems in the same IP zone will always connect on IP as default when they are booked via TMS, so if you always want to use ISDN between systems in a location – they should not be part of an IP zone. An example; systems that will never connect on ISDN (except through a gateway) should not be part of an ISDN zone.

2.1 ISDN Zones

To set up an ISDN Zone simply click the 'New' button and fill in the following fields:

ISDN Zone Name:
Specify the name of the ISDN zone

Country/Region:
Choose the country this zone is situated in. This will let TMS choose the correct country code and correct international dialing prefixes.

Area Code:
Specify the area code this zone is situated in. This will let TMS choose the correct area code rules

To access an outside line for local calls, dial:
Insert the prefix needed to gain an outside line in this ISDN zone

To access an outside line for long distance calls, dial:
Insert the prefix needed to gain an outside line for long distance calls in this ISDN zone. NOTE that if you use the same prefix to gain an outside line for both local and long distance calls you should put the same prefix here as you put in the previous field.

Number of digits to use for internal ISDN calls:
This specifies the number of digits used for internal dialing within this zone. The leading digits will be stripped from the number when dialing between systems in this ISDN zone.

Note:
If TMS is generating the wrong numbers to dial when dialing local, domestic or international calls, you should have a look at the ISDN zone settings and the phone number set on the system.

Example:
A Swedish phone number in Stockholm would have a number layout like this:
Country code (+46)
Area code (08)
Local number (12345678)

- If dialing this number from within Stockholm they would only dial the local number: 12345678
- If dialing from Gutenberg (within the country, but outside the area code) they would dial: 08 12345678
- If dialing from outside Sweden they would dial: +46 8 12345678

As you see the 0 in front of 8 (in the area code) would have to be removed when dialing this number from outside the country. This is therefore not looked upon as part of the area code, but rather a prefix to dial between area codes.

The systems should only be configured with the local ISDN number: 12345678, but with the correct area and country code in the ISDN Zone. If the system was wrongly configured with the local number and the area code, TMS would wrongly configure the following as the international number for the system: +46 8 0812345678

In the ISDN Zone the area code should be stored as just 8, since TMS will add a 0 in front of it when dialing between Swedish area codes, and add +46 when dialing from outside Sweden.

There are some exceptions to these rules, but TMS are aware of them.
- Some countries like Norway do not use area codes; hence the area code field in the ISDN zones in these countries should therefore be left empty. E.g. +47 12345678
- Some other countries like Italy include the leading zero in the area code even when being dialed into from outside the country. This means that the area codes in the Italian ISDN zones should include the leading zero. E.g. +39 02 12345678
- Other countries again such as Switzerland include the area code with the leading zero when dialing within an area code and when dialing within the country, but remove the leading zero when being dialed into from outside the country. TMS knows this so the area code for ISDN zones in Switzerland should only include the area code without the leading zero. E.g. +41 33 1234567 and 033 1234567

2.1.1 Area Code Rules

Area code rules are typically used in the US to set up 10-digit dialing and area code overlays. Area code rules determine how ISDN-numbers are dialed 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'-button inside the ISDN zone. After clicking the link, a page with an overview of all area code rules for the ISDN zone is displayed.

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 by pressing the 'Edit' links to the right of every rule, or deleted by checking the rule and clicking the delete button.

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 dialing 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:

When dialling from this area code to the following area code (Field 1):
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.

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

Include Area Code:
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 dialing.

Before dialing, also dial:
If the rule applies, as stated in Field 1 and Field 2, the digit(s) in this field will be dialed 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 ISDN zone.

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

2.2 IP Zones

To set up an IP Zone simply click the 'New' button and fill in the following fields:

IP Zone Name:
Specify the name of the IP zone

2.2.1 Gateway Resource Pool

ISDN Zone:
Below you will specify which prefixes to dial, in order to use a gateway. The ISDN Zone dropdown allows you to specify which ISDN Zone's dialing rules that should apply to the gateway you will use. The reason why you specify the prefix to use, rather than the gateway directly is to allow more flexibility in TMS – since you then can use load balanced gateways, and even gateways not supported by TMS.

Note: This setting must be set in order for the Gateway Resource Pool to work.

URI Domain Name:
Add which domain name TMS should use for routing H323 calls to this IP-zone when doing URI dialing.
NOTE. TMS will always use URI dialing between two locations where this setting is filled in – thereby ignoring the IP/ISDN preferences defined at the bottom of this page.

Gateway Auto Prefix:
Set what prefix should be used to get an outside ISDN line through the gateway for video calls.

Gateway Telephone Prefix:
Set what prefix should be used to get an outside ISDN line through the gateway for telephone calls.

Gateway 3G Prefix:
Set what prefix should be used to get an outside 3G line through the 3G gateway for 3G calls.

Dial-in ISDN Number:
Specify the TSC4 number that will be used for dialing into endpoints through a gateway. TMS will automatically generate the entire number for a call; containing the gateway's TSC4 number followed by the star and the endpoint's E164 alias.

Dial-in ISDN Number for 3G:
Specify the TSC4 number that will be used for dialing into endpoints or MCUs through a 3G gateway. TMS will automatically generate the entire number for a call; containing the gateway's TSC4 number followed by the star and the endpoint's E164 alias.

Allow IP-ISDN-IP:
Check this option to allow TMS to schedule calls from an IP only endpoint out through an IP-ISDN gateway to an IP only endpoint in via an ISDN-IP gateway. The set-up time for this type of calls can be close to a minute.

Prefer IP calls to specific IP zones:
Systems in the same IP zone will always prefer to dial each other on IP. This will be the preferred call option when booking via TMS booking and the only option when using a different booking interface like Outlook, Lotus Notes, Microsoft Office Communicator, Lotus Sametime or TANDBERG Scheduler. The systems in the same IP zone will be dialed on E164 alias if all systems in the conference are registered to one gatekeeper or different neighboring gatekeepers. Participants that are not reachable through a gatekeeper will be dialed to (or from) with IP-addresses.

By moving IP zones between the two lists at the bottom of an IP zone, you can specify which IP zones should be dialed using IP, and which IP zones should be dialed using ISDN.

When setting up a conference with participants in different IP zones, TMS will try to include a MCU from the IP zone where the majority of the participants are situated.

3 Adding Systems

Systems in TMS include Endpoints, Gateways, Gatekeepers, MCUs, Equipment and Rooms. Every system can be represented in multiple folders, but they will all have the same entry in the database – which means that changes done to the system will be reflected in all the representations of the system.

3.1 Automatic system discovery

In TMS 11.5 a new feature called 'Automatic system discovery' was added. This feature can be turned on during installation or after installation by going to 'Administrative Tools → Configuration → Network Settings'. When turned on TMS will scan the network for systems, and if a rouge system responds (a system not yet known to TMS) this system will be automatically added to a default folder, and given a default template that will include an IP-Zone and a TMS Phonebook containing all the endpoints in TMS. The folder and template can be changed under 'Administrative Tools → Configuration → Network Settings'.

3.2 Add Systems

On this page you have 4 different Tabs where you can add systems to the specific folder in TMS where you are standing. Each of them allows different ways of adding systems and rooms/equipment:

Add Systems:
On this page you may either enter a start IP-Address and a end IP-address for a range of systems to be added, or you may enter a comma separated list of IP-addresses and host addresses for those systems you wants to add to the TMS. The following example will add two systems, one by DNS name and one by IP address, and scan ten systems in a range: "user.tms.int, 10.0.0.1, 10.1.1.0 - 10.1.1.10"

You should also on this page specify the correct locations for the systems, and the time zone. In the advanced area you can:
- Enter username, password and/or an admin password if the systems require it in order to be added.
- Select a template to be set as persistent settings on the systems.
- Set discovery options, like which SNMP names to use when searching for systems, if you want to search for non-SNMP systems and whether or not to add discovered system although they are not supported by TMS (like PC's and network infrastructure devices). The list of SNMP community names is pulled from Administrative Tools → Configuration → Network Settings → SNMP Community Names. If you know the community names of the system you want to add you may edit this field to speed up the adding process. Any changes here will NOT affect the settings under Administrative Tools.

From List:
On this page you can add systems that have already been added to TMS (that are not already in the current folder) or have been automatically discovered by the TMS Network Scanner by

checking of the checkbox to the left of the systems. You should also specify the locations and the time zone you want the systems to have.

Pre Register Systems:
If you are planning to deploy a large number of endpoints, pre-registering them allows TMS to configure them when they become online the first time. When you pre-register, you must supply a name for the system and an identifier. You must first select what to use as primary identifier (MAC address, IP, Serial number) for the systems. Please note that currently only TANDBERG MXP series supports using serial number as identifier. TANDBERG recommend using MAC address as the unique identifier for systems. If you want a list of settings to be applied to the system when it comes online, you can select a pre-created template from the list. This template can be modified any time through the template pages. A persistent template for the system can also be preconfigured here, together with the option of setting persistent e164 alias, h323 id and the endpoint name. The templates and persistent settings require that the system supports templates in TMS.

Add Rooms/Equipment:
On this page you select if you want to enter a room or a type of equipment. Then enter the name of the room or equipment you want to add to the TMS. If you select to add a room you are able to set more settings in the advanced area. In the advanced area you may enter information about IP, ISDN, Gatekeeper, SIP and location settings.

When adding systems and rooms/equipment, TMS will analyze the systems configurations using the ticketing service to ensure that when a system is added its settings are verified. If TMS finds any faulty configurations it will present the system in the table with the header saying "NOTE: Systems Discovered with Incorrect Settings, Not Yet Added to Folder:", and with a description in the row in the table saying what is wrong. You may change / correct the settings by clicking on the "Edit" link in the row in the table where the system is presented. In the page that is popping up, if you decide to change the settings you may update settings on the video conferencing system, so please have the manuals for the systems available.

If there are no incorrect system settings, the system will be added to the folder and will be shown in the table saying "Systems Discovered and Successfully Added to Folder:".

If the system is already added to the folder, you will get a message saying that it already is in the folder. The system will be added to the table saying "Systems Discovered and Successfully Added to Folder:"

If the system couldn't be added because the SNMP Community Name is not added to the list in TMS, or TMS couldn't get in contact with the system or the system is of a type that TMS is not supporting, it will be added to the table saying "NOTE: Systems That Could Not Be Added:".

3.2.1 Adding a TANDBERG Content Server

TMS 11 supports adding the TANDBERG Content Server (TCS) for booking and management purposes. When adding the TCS to TMS follow the procedures above, but also check the "Discover Non-SNMP Systems. WARNING: Will significantly increase time required for discovery" checkbox in the Advanced section of the Add Systems page.

Note: TMS 11.0 and TCS version 1.0 only support booking calls with the transcoding line on the TCS.

3.3 How pre-registration works

When pre-registering a system, you can select whether you want the system to be identified on 'Serial Number', 'MAC Address' or 'IP/Hostname'. Please note that only the TANDBERG MXP endpoints can pre-register based on Serial Number. Another thing that is important to keep in mind is that only systems supporting SNMP can be pre-registered by serial number and MAC-address if they are using static IP addresses. TANDBERG MXP endpoints are using HTTP traps rather than SNMP traps to communicate with the TMS server for most information. They are therefore dependent on having their External Manager's IP address configured. This is done automatically when the endpoint contacts the DHCP server to retrieve an IP address, but only if the option 242 on the DHCP server is configured to point to the TMS server.

3.3.1 Configuring the DHCP server

If you are using a Windows 2000/2003 DHCP server, add the following settings in the DHCP Manager:
You can create the 242 option by redefining an existing global option. To do this, highlight the global option in the "Unused" list and click on **Add** in the DHCP manager. Once you have defined a vendor-specific option, you can select it for use by the vendor class by moving the option to the "Configured" list, and defining its value which should be the IP or the DNS name of the TMS server.

If you are using ISC's DHCP-server, put the following statements in *dhcpd.conf*.

First define option 242:
option local-tms-ip code 242 = ip-address;

Then define the value in the subnet of pool section:
option local-tms-ip < IP address>;

If the systems are not using DHCP they need to be able to respond to the SNMP broadcast messages that TMS will send out on set intervals. This interval is configurable in Administrative Tools → Configuration →Watchdog.

NOTE: The TANDBERG 150 MXP with L1.1 and L1.2 is configured to request the DHCP for option 173. It is therefore advised to either upgrade the endpoints to a newer software, or to configure both the option 242 and 173 on the DHCP server until the endpoints are upgraded.

3.4 Persistent Settings

Persistent settings are settings that allow the administrator to enforce settings on systems throughout the network. These persistent settings can be specified during pre-registration or after the system has been added to TMS (via the persistent settings tab in Navigator).
The persistent settings will be set on the endpoint every time TMS receives a boot event from the endpoint; either via SNMP or HTTP.
There are four persistent settings; Three of them allow you to set a persistent System Name, H323 Id and E.164 Alias. The last setting gives you the option to pick a predefined template that will be set on the endpoint after every system boot. The template can typically include settings like "auto answer on", "microphone off" and "Volume 7"

3.5   How to best swap a system in TMS

Systems get an id (TMS System Id) when they are first added to TMS. This id is used as the reference for the systems in booking, reporting, event, permissions etc. It is therefore important to retain the id, even if a system gets swapped (because of theft, upgrade, hardware failure etc). A system should therefore "never" be purged from TMS. It may be deleted from a folder since the data for the system will still be in the database, but it should not be purged unless you are 100% confident that a new system should take over this system's roles.

If a system in TMS is out of order, or awaiting a swap, it can be set to not *Allow Bookings*. This is done in the *Connection* tab in Systems - Navigator. By doing this you can avoid anyone booking the system while it is unavailable.

3.5.1 Replace system function

In TMS 11.5 a new feature called 'Replace system' was introduced. This feature makes it much easier to replace systems in TMS and should be used to replace systems in TMS.

When replacing a system, go to Systems → Navigator and find the system you wish to replace. When the system summary page has opened, click the 'Connection' tab followed by clicking on the 'Replace Systems' link. Here you choose whether to change the system's network address to an IP or DNS address of a system on the network, or choosing an existing system in TMS by clicking the 'Select system…' button. When this is done, you click the 'Next…' button. You will then be shown a summary page where you choose whether you would like to keep the system name, keep call configuration, apply last configuration backup and keep all logs of the system. You can also choose to purge the system that you are replacing from TMS. When you have made your choices, click the 'Ok' button and the switch will be completed.

3.5.2 System tracked by IP address

When a system is tracked by IP address and the system is swapped, the easiest way is to give the new system the same IP address and connect it to the network. If a *Configuration Backup* was done of the previous system, a *Configuration Restore* can now be done to restore all previous settings and phonebooks.

If the new system is configured with a new IP address, then insert the new IP address in the *Connection* tab for that system in *Systems – Navigator* in TMS and press the *Save/Try* button.

Note: Verify that the SNMP community name is correct, or else this will not work.

3.5.3 System tracked by Host Name

When a system is tracked by the Host Name and the system is swapped, the new system should be configured with the same host name. If a C*onfiguration Backup* was done of the previous system, a C*onfiguration Restore* can now be done to restore all previous settings and phonebooks.

If the new system is configured with a new Host Name, then insert the new Host Name in the *Connection* tab for that system in *Systems – Navigator* in TMS and press the *Save/Try* button.

Note: Verify that the SNMP community name is correct, or else this will not work.

3.5.4 System tracked by MAC address

When a system is tracked by MAC address then TMS relies on traps from the endpoint containing the (new) IP address of the system and the MAC address. If the IP address has changed (which happens when using DHCP), then TMS will update the IP address in the database to the new IP address. TMS will then be able to contact the system.

When swapping a system with a new system, the MAC address will change. So if TMS is tracking the system by the MAC address, the MAC address in TMS needs to be updated. This can be done in two ways:
1. Update the MAC address field in the *Connection* tab for the system with the new system's MAC address, click *Save/Try*, and reboot the system via the remote control or telnet. This will make the endpoint send a trap to TMS with its MAC address and IP address – resulting in TMS recognizing the MAC address and updating the IP address in TMS.
1. Set the *Track system on network by* option to *IP Address* and update the IP address to the new IP address of the system. Click *Save/Try* to allow TMS to read the new MAC address, and set the *Track system on network by* option back to *MAC Address*.

If a C*onfiguration Backup* was done of the previous system, a C*onfiguration Restore* can now be done to restore all previous settings and phonebooks.

Note: Verify that the SNMP community name is correct, or else this will not work.

4 Support for remote systems

From TMS 11.5, remote systems are supported for booking, getting software upgrades, receiving phonebook and be part of the statistics that is created in TMS. The following section will cover how this feature works and answers to some frequently asked questions.

4.1 How the communication works

A remote system can be either located publicly on the Internet or behind a firewall. The way TMS communicates with these two differs slightly.

1) Reachable on public Internet
   ▪ Having the system set to 'Reachable on Public Internet' as 'System Connectivity' will make TMS communicate with the system in the same way as it does with the systems internally. However, since the system cannot contact TMS on TMS's internal DNS name or IP address, TMS will set a different address for the phonebook service and feedback on the endpoint. The addressed used is the one listed under 'Administrative Tools → Network → Advanced Network Settings'.
   ▪ When the system is reachable on the public Internet you can have TMS communicate with the system on both HTTPS (port 443) and HTTP (port 80).
2) Behind firewall
   ▪ Setting 'Behind firewall' as the 'System Connectivity' will make TMS communicate with the endpoint in much the same way as 'Reachable on Public Internet', except TMS will not be able to tell the endpoint to dial and must therefore set up a route where i.e. an MPS is calling to the endpoint.
   ▪ All communication between the system and TMS will be HTTP over port 80.
   ▪ The connectivity method will only work if the system is behind a firewall or router that uses NAT.
   ▪ TMS will automatically detect that a system is a SOHO system when the IP address the endpoint reports in status.xml is different from the IP address the HTTP packets are coming from, and the set the 'System Connectivity' to 'Behind Firewall'.

When a system is plugged in at a remote location it will contact TMS either with a register event or a boot event (dependent on if the system is already in TMS – see 4.2). When TMS gets this event it will reply with an acknowledgement and ask to get three files from the endpoint: 'status.xml', 'history.xml' and 'configuration.xml'. In addition it will check if any software upgrade has been scheduled for the endpoint, and if so perform this. After 60 seconds, the system will communicate with TMS which will set the feedback expression on the system enabling it to send events. TMS will also set the endpoint to contact the TMS server every 15 minutes. This will be the heartbeat that allows for the communication between the TMS server and the remote system, and any change that is done on the remote system or in TMS will be synchronized through this heartbeat.

We recommend that the remote system is on a DNS compatible network to ensure proper communication between TMS and the remote system.

4.2 Adding a remote system to TMS

Before you can use a system as a remote system in TMS, you must be sure to have set a public DNS address on the TMS server. This can be done under 'Administrative Tools → Configuration → Network Settings'.

4.2.1 A system already added to TMS

The easiest way to add a remote system to TMS is to first have the system registered in TMS before you bring it home. Before you unplug it you go into the 'Connection' tab on that endpoint and change System Connectivity to 'Behind Firewall'. TMS will then set the management address on that system to TMS' external management address. When the system is plugged in at home, the system will then send a boot event to TMS and from then on the system will be available from TMS.

4.2.2 A system not added to TMS

If you want to use an endpoint that has not been added to TMS before it is plugged in at the remote location, you will need to set the external management address of TMS on the endpoint. This can be automatically done by the DHCP server (ref chapter 3.3.1) or manually on the endpoint. With F5.x and L4.1 this must be done using telnet, while F6.x and L4.2 (and newer) has this in the endpoint's menu:

1) In Windows, press Start and Run.
2) Type 'telnet <ip-address of the endpoint>' (This can be found on the endpoint by pressing the Up arrow and then the Left arrow)
3) Type password if needed
4) Type 'xConfiguration ExternalManager Address: "<dns name of the TMS server>"' or if using a proxy the dns of the proxy server.
5) This configuration is correct by default, but if it has changed then type 'xConfiguration ExternalManager Path: "tms/public/external/management/systemmanagementservice.asmx"'
6) Type 'bye'

When this has been set the endpoint will send a register event to TMS, and when TMS receives this and notices that the system is not already in TMS, it will add it to a list and one must add the system to TMS afterwards. However, if automatic system discovery has been enabled, the system will be added in the default folder specified in the 'Administrative Tools → Configuration → Network Settings'.

4.2.3 Setting an endpoint in public

If your system is not behind a firewall and put in public instead, it is advised to change the system connectivity on the system to 'Reachable on Public Internet'. This way it will also be possible for TMS to set up calls where the endpoint is calling out, and not only being called to.

4.3 Booking

A booking in TMS including remote systems can be done like any other booking. However, as TMS is not able to communicate directly to the remote system that is behind a firewall, it is

not possible for TMS to ask the endpoint to initiate a call. The endpoint must therefore be dialed into. If two or more remote systems that are behind a firewall would like to call each other, an MCU or a system with multisite (Will only be included if booked in the call) that is located internally would therefore have to be needed to set up the call.

4.4 Phonebooks

The phonebook will work in the same way as if the system was located on a LAN. When the endpoint is requesting the phonebook it will send the request to the TMS server where TMS creates the .xml file and sends it back to the endpoint as the response.

4.5 Software upgrade

Software upgrade on remote systems is set up in the same way as software upgrade on internal systems. However, the mechanism used to upgrade the system is different. When you have scheduled the upgrade TMS will say that the upgrade went successfully. What has happened is that TMS has put the upgrade on hold until it gets a **boot** event from the system. When TMS gets this boot event, it will see that an upgrade has been scheduled for that system and on the reply to the boot event TMS will send the endpoint an URL where it can get the software package. This URL is defined under 'Administrave Tools → Network' in the 'General Network Settings' panel. It is recommended that the directory is left to the default (tms/public/data/software) as this is where TMS populates its list of packages from (Systems → System Upgrade → Software Manager). In other words, if you provide a different URL you might end up scheduling an upgrade with a package found in the list that is not found in the URL specified.

4.6 Statistics and monitoring

The statistics and monitoring of the remote systems will be made up the same way as systems that are on the LAN, by sending event traps to TMS. As for retrieving status and detailed call information ('status.xml' and 'history.xml'), these ones are sent every 15 minutes. The configuration of the system ('configuration.xml') will be sent by demand (Pressing 'Force Refresh' in TMS) or when doing changes in TMS.
Ad-hoc calls will not be shown for systems behind a firewall as the TMSLiveService service is not able to contact the system to get information about the call.

4.7 TMS configuration

To allow for the remote systems to communicate with the TMS server, TMS needs to be reachable from the remote system. There are several ways that this can be done:

1) Put the TMS in public
   - o This option is the one that provides less security, and makes the TMS vulnerable for attacks directly over the Internet.
2) Put the TMS in DMZ
   - o This option provides a bit more security. Port 80 (HTTP) needs to be open in the firewall to allow for incoming traffic.
3) Use a proxy

o   This option provides the best security without having to have two separate
       TMS servers, and is set up by having the proxy forward to the TMS server
       requests that are made to the management address path of the TMS server.
       i.   /tms/public/external/management/systemmanagementservice.asmx
       ii. /tms/public/feedback/code.aspx
       iii. /tms/public/external/phonebook/phonebookservice.asmx
       iv. /tms/public/feedback/postdocument.aspx

4) Have two TMS servers, one on the inside and one in DMZ talking to the same
    database
       o   This will allow you to add and manage the internal and external systems
           seamlessly, but requires some extra configuration of firewalls and the external
           TMS server.
       o   The TMS server in the DMZ should only be accessible on port 80 from the
           Internet, and can also be limited to only respond to the connections, but not
           open any new connections. The TMS in the DMZ must be able to talk to the
           SQL server on the inside of the network, but this can be limited to one port
           only. It is recommended to use a limited user with only read/write permissions
           to the *tmsng* database for this (doing upgrades of the TMS server will require
           db_owner permissions to the tmsng database), and to disable the
           XP_CMD_SHELL command on the SQL server for security reasons.
       o   All TMS services on the TMS in the DMZ must be disabled to prevent the
           TMS in the DMZ from trying to contact systems on the inside.

5) Have two TMS servers, one for internal and one for public systems
       o   This is the most secure option, but will remove some of the features as well as
           complicate the usage. The booking will be limited since internal and external
           systems are now in two different databases. The two databases will also cause
           a problem for statistics as the remote systems will have its statistics stored on
           the public TMS and the internal systems will have its statistics stored on the
           internal TMS. System upgrade will need to be scheduled separately, and
           software packages must be put on the two servers. Phonebooks can however be
           centralized using a LDAP server that is available for the two servers (see
           chapter 6)

5 User permissions

5.1 User Administration

User Administration controls which users have permissions to which parts of TMS. Permissions are controlled on a group level (i.e. you assign permissions to a group). The total permission level for an end user will then be the sum of all the permissions assigns to all the groups that the end user is a member of. Note: An end user can be (and in most cases is) 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 the rights to edit the 'Configuration pages' under 'Administration Tools', i.e. only Site Administrators can change the IP address of the server and alter the option keys.

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 the rights to edit the 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 organization to have. This applies to both what TMS functions you want them to see, as well as which systems they are allowed to use.

*Note that you are not allowed to change any of the permission rights for the Site Administrator group. Also, you cannot add or remove users belonging to the **Users** group as all users by default are members of this group.*

5.1.1 User Information and preferences

A new user is automatically added the first time the user accesses TMS, as the Windows Username of the user is automatically detected. If configured in the Administrative Tools → Configuration → Network Settings page, TMS will also try and detect new user information such as email address, first and last name through Active Directory lookup. If the information is not available the user will be prompted to fill in user information and user preferences, as listed in the table below, in a popup window. First and last name and email address must be filled in at first time log on to the TMS server.

User Information and preferences

Windows Username	Your username on the TMS server. This is automatically detected by the Internet Information Server. This information can only be changed by an administrator
First Name	The users first name
Last Name	The users last name
E-mail Address	The email where meeting bookings and event notifications will be sent to. The format must be on the form xxx@yyy.zz.
Language	This option lets the users select between 15 different languages in TANDBERG Scheduler where 3 of the languages also affect the rest of TMS (English, Simplified Chinese and Japanese.) English is the default language for TMS, i.e. if a user selects Swedish as the language he or she will get the Scheduler presented in Swedish and the rest of the TMS in English.
Office Telephone	The users office telephone number
Mobile Telephone	The users mobile telephone number
Primary System	The users preferred video system.
Web Conference Username	The username for accessing the web conference account
Web Conference Password	The password for accessing the web conference account
SIP URI:	This is the SIP URI of the user. This field is used by the TANDBERG LCS integration. The SIP URI is automatically retrieved from AD if the AD lookup is properly configured in TMS.
Time Zone	This option is used to present the correct time and date information for the users in TANDBERG Scheduler (if the client is on a different location than the TMS server).
Location	This field allows the user to select an IP zone where the user is situated. This IP zone is used when a user books a meeting with only dial-in participants, to ensure that the MCU that is closest to the user is picked.
Number of last used systems listed	This option lets the user choose how many of the previously used systems should be shown when booking a meeting in TMS.
First page for New Conference in Scheduler	Lets the user choose if he/she wants to start with the "default page", the "choose conference room page" or the "choose time page" when opening Scheduler.
List your meetings when opening TANDBERG Scheduler	Lets the user choose if all their meetings should be listed when accessing TANDBERG Scheduler

5.2 Limiting access to TMS / Locking out a set of users

TMS is running on top of Microsoft Internet Information Server and is therefore also utilizing the Windows user structure for authentication. If the TMS server is part of a domain, TMS will look up any new and existing users in the Active Directory or the local users to see if the users have the proper permissions to access the TMS server. If the user has access to the server, they will also get access to TMS, and automatically become members of the user groups defined in 'Default Groups'. When TMS is installed the first time, all new users will become members of the 'Site Administrator' group – which is something that should be changed as soon as possible. By setting the 'Default Groups' to 'Users' and limiting the access of the group 'Users' you can deny access to TMS to all new users, even if they are allowed to access the server through the user permissions. A 'Video Unit Administrator' can then grant each new users the proper permissions by adding them to a new custom defined group.

5.3 Groups

This is where you view, edit and set permissions TMS user groups.
To add a new group press the 'New' button, fill in the name of the group and a description for this new group.

TMS supports using AD groups where the group memberships for users are managed through Active Directory. AD groups must first be enabled in the 'Administrative Tools → Configuration → Network Settings page', and the AD lookup information must be configured with a Domain user. AD groups can then be imported to TMS and given permissions to as a normal TMS group. TMS will do a lookup towards AD during login for every user to see which AD groups they belong to, and give them the respective permissions in TMS.

Select which users should be part of the group if the group is not an AD group, and press 'Save'. To set the permissions for a group, click on the 'Set Permissions' link. A page with multiple checkboxes will then load. To set permissions for the users in a group checkboxes must be checked and 'Save' pressed. When setting up permission choices for user groups' access to different parts of TMS, the following permission choices are available:

5.3.1 Portal

Portal Page: If the "Read" permission is checked, then the users of this group have access to see the Portal Page.

Sitemap: If the "Read" permission is checked, then the users of this group have access to see the Sitemap.

5.3.2 Booking

List Conferences – All: Decides if the users of this group have access to "Read" the page, "Create" new meetings, "Update" a meeting, "Delete" meetings and / or "Export" the list of meetings to an Excel sheet.

List Conferences – Mine: Decides if the users of this group have access to "Read" the page, "Create" new meetings, "Update" a meeting and "Delete" meetings.

List References:
Decides if the users of this group have permissions to Read and/or update (add new, edit or delete) References.

Participant Templates:
Decides if the users of this group have permissions to Read and/or update (add new, edit or delete) participant templates.

Misc: If the Booking checkbox is checked, then the users in this group will have access to the booking pages "Book a meeting" and "Free Busy Overview". Be aware of that there are additional permission levels related to individual systems and the folders they are in. If the user has access to All Meetings "Create" the user has access to book the system regardless of system settings.

If the Ac-Hoc Booking checkbox is checked, then the users will have access to this page.

If the Scheduler checkbox is checked, then the users will have access to this page.

If the Advanced Settings checkbox is checked, then the users will have access to the Advanced Setting page in TANDBERG Scheduler.

If the Approve Meeting is checkbox is checked, then the users have the opportunity to approve or reject scheduled meetings. If this checkbox is not checked, all the meetings booked by a user in this group will need their meetings approved by a user that has this permission.

5.3.3 Monitoring

Misc:
These checkboxes limits which monitoring pages the users should be able to see.

5.3.4 Systems

Navigator:
Specifies if users should have access to the System navigator, and/or be able to purge systems from the database

Ticketing Service:
Specifies if the users should be able to use the Ticketing Service

System Overview:
Specifies if the users should be able to make system overview reports

Manage dial plan:
Specifies if the users should be able to see and change settings from the 'Manage Dial Plan' page

Configuration Backup:
Specifies if the users should be able to make backup and/or restore jobs – and see the status of these jobs

Provisioning:
This setting defines if the users of this group should have access to "Read" the page, "Create" new templates, "Update" templates and "Delete" templates.

System Upgrade:
The users in this group will have access to the listed pages by checking the checkboxes beside the page name.

Purge Systems:
Specifies if the users should have access to purge systems from the database

Network History:
Specifies if the users should be allowed to see the network history in TMS

Event Notification:
This setting defines if the users of this group have "Read" access to this page, "Update" (edit) the Event Notifications for all users, or only Update / Edit "Own Notifications".

5.3.5 Phone Books

Phone Books:
This defines if the users of this group should be able to "Read" this page, "Create" new phone books, "Update" a phone book, "Delete" phone books, "Set On System the phone book, "One-time Import" a phone book and "Connect To External" sources.

External Sources:
This setting defines if the users of this group should be able to "Read" this page, "Create" new external sources, "Update" an external source and "Delete" external sources.

5.3.6 Reporting

Reporting:
Specifies which components under reporting the users should have access to.

5.3.7 Administrative Tools

Configuration:
This setting defines if the users of this group should be able to "Read" this page and "Update" the configuration settings.

Users:
This setting defines if the users of this group should be able to "Read" this page, "Create" new users, "Update" a user, "Delete" users and "Set Groups" that the user shall be a member of.

Groups:
Decides if the users of this group should be able to "Read" this page, "Create" new groups, "Update" a group, "Delete" groups, "Set Permissions" that the group members shall have and "Set Default Group" that all new users in TMS automatically becomes members of.

IP Zones:
Decides if the users of this group should be able to "Read" this page, "Create" new IP Zones, "Update" an IP Zone and "Delete" IP Zones.

ISDN Zones:
Decides if the users of this group should be able to "Read" this page, "Create" new ISDN Zones, "Update" an ISDN Zone and "Delete" ISDN Zones.

Billing codes:
Specifies which part of billing codes the users should have access to managing.

Activity Status:
This setting defines if the users of this group shall have "Read" permission to this page, and if he/she should be able to "Delete" an Event Log.

TMS Server Maintenance:
This setting defines if the users of this group shall have "Read" permission to this page.

TMS Tickets:
Specifies if the users should be able to see the TMS tickets

Audit Log:
Specifies if the users should be able to see and search in the audit log.

5.4 Users

A list of all the registered users is listed. From here, new users can be created and existing users can be edited or deleted. Selecting 'New' 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 'Save button to store the user's data.

Notes: Users must be members of the Windows Network to be able to be users of TMS.
You cannot delete your own user representation nor edit your own 'Windows username' while logged on.

5.5 Default Groups

Default groups define which groups a new user automatically will be assigned to when logging into TMS for the first time. 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 simply choose the wanted groups and click on the 'Save' button.
If you wish that users by default should not have access to TMS you have two options:
- Change the settings in the Active Directory so that those users don't have access to log into the TMS server
- Remove all the permissions from the Users group and set this, and only this, group as the default group. All new users on the TMS server will then be denied access to TMS. You should then create an additional group with the minimum permissions would want a trusted user to have. These users needs to be added into the group after they log into TMS the first time (so that the user is created), or you could predefine the users in TMS and put them in the group. The next time a user logs in, the username will be matched with the one already configured.

5.6 Default System Access

On this page you can define which permissions should automatically be applied to systems added to TMS. These permissions can be adjusted at a later time by going to Systems → Navigator. There are defined five different access levels to folders and systems. These are: Read, Book, Edit Settings, Manage Calls, and Change Permissions. You can set these permissions based on the different access groups in TMS.

6 Phone Books

There are three types of phone books available on TANDBERG endpoints:

6.1 Local Directory

The local directory is a file stored on the endpoint made by entries inserted through the remote control on the endpoint. It's not touched by TMS, but can be imported into TMS' phone books as an external source

6.2 Global Directory

The Global Directory is a file stored on the codec where the entries cannot be changed via the remote control. The file is transmitted to the endpoint over FTP to all endpoints that are "subscribing" to one or more phone books in TMS. Multiple phone books will be merged into one phone book (and if containing more than 400 entries, only the first 400 will be shown on the endpoint). The file will be transmitted to the endpoint on the intervals set in the "Update Frequency" setting in "Set on Systems" under phone books.
Note: Only works on the endpoints supporting the globdir.prm file.

6.3 Corporate Directory

The Corporate Directory is a XML service on the TMS server that allows the endpoint to retrieve the phone books directly from the server every time the phone book button on the endpoint is pressed. It allows for a hierarchy of phonebooks and multiple phone numbers on every entry. The Corporate Directory is also searchable.

6.4 Setting phone books on systems

There is a global setting in TMS (Administrative Tools → Configuration → General → TANDBERG System Phone Books) that allows administrators to select if Corporate Directory, Global Directory or both should be used in their network. Using both is recommended since this will give the endpoints a failover option – if TMS is not reachable and the Corporate Directory cannot be displayed, the Global Directory will show the 400 first entries in a flat list.

To select which systems should get the different phone books go into Phone Books in TMS, click the 'Set on Systems' link on a phone book, and select which endpoints should get this phone book.

   – Endpoints supporting both the Corporate Directory and the Global Directory will have their Corporate Directory settings adjusted to point to the TMS server, and have the Global Directory (the globdir.prm) file transmitted to the endpoint over ftp at three different events:
      a. every time adjustments to the 'set on system' list is made
      b. at the intervals specified in the 'Update Frequency' dropdown menu
      c. by a background service that by default will run every 4th hour if "Enforce Management Settings" is turned on (Administrative Tools → Configuration → Network Settings → Enforce management settings on systems).

‒   This globdir.prm file will then be available if the TMS server is offline. The entries will be showed together with the local entries on the endpoint.
     Endpoints such as TANDBERG MXP and TANDBERG Classic (E4/B9 or newer)

‒   Endpoints only supporting the Corporate Directory will only have the Corporate Directory settings set on the system. This will happen every time a change is done to the 'set on system' list, and at the intervals specified in the 'Update Frequency' dropdown menu.
     Endpoints such as TANDBERG 150 MXP with L1.x or L2.x software and TANDBERG 3G Gateway

‒   Endpoints only supporting the Global Directory (globdir.prm) will have the Global Directory (the globdir.prm) file transmitted to the endpoint over ftp every time adjustments to the 'set on system' list are made, and at the intervals specified in the 'Update Frequency' dropdown menu.
     Endpoints such as TANDBERG Classic (E3.x/B8.x and older) and TANDBERG MCU (D 3.x or newer)

Settings that will be set on the endpoints supporting Corporate Directory:
(xconfiguration) corpdir mode on
(xconfiguration) corpdir ipaddr x.x.x.x (server's IP address)
(xconfiguration) corpdir path TMS/Public/external/phonebook/PhoneBookService.asmx

7   TMS features

7.1 Operator Conference

From TMS 11.5 Conference Control Center now supports the concept of Operator Conferences. Operator Conferences are ad-hoc created conferences that can be used by conference operators to work with individual participants of a conference outside their normally scheduled call. If a site is having a problem, or has questions, an operator can now start a new conference and add themselves and the problem site(s) to the special conference. When the operator is done, the Operator can send the site back to their originally scheduled call. All of this is one easily with simple clicks from TMS's Conference Control Center.

TMS's Operator Conference features:
• Create Operator Conferences on the fly with a single click
• Simple click on participants to move to an operator conference without disconnecting the site
• If no Operator Conference exists, a new one can be created automatically
• Operator's can have a default system for themselves that can be automatically added to the conference when an Operator Conference is started
• Operators can move a participant, or multiple participants in and out of an Operator Conference at will from Conference Control Center
• Multiple Operator Conferences can be running simultaneously
• Participants moved to an Operator Conference are still shown as participants in the scheduled meeting but with special icons to show them as moved
• Operator Conferences will automatically clear themselves out if no longer used by the Operator's system

7.1.1 How to set up an operator conference

To be able to set up an operator conference you need to have TMS 11.5 and an MPS with J3.0 or later, and the conference must be hosted on that MPS.

When viewing the conference in Conference Control Center, you can move a participant out to an Operator Conference by first selecting the participant from the participant list and

clicking the 'Move to Operator Conference' button ![button] or right-click on the participant and choose 'Move to Operator Conference'. Afterwards, a window will pop-up allowing you to choose a system that you want to use as operator system and also if you would like the new conference to use encryption. When you have made your selection, click OK and the operator conference will be created.

Note that the participant will only be moved out of its conference when the operator is successfully connected to the operator conference, stopping the possibility for the participant to be moved into an empty conference.

To end the operator conference, select the participant from the operator conference and click

the 'Move back' ![button] button or right-click the participant and choose 'Move back' or from

the main conference select the participant and click the 'Get back' button ![button].
If the Operator Conference is not ended, the operator will still be in the conference, thereby saving connection time if a new participant is to be pulled into the operator conference.

---

8 Troubleshooting the TMS components

This chapter will go through the different components that TMS consists of. The five services that should be running at all times, the Java applet needed to show the monitoring pages, the web server needed to display TMS as web-pages and the database were all information is stored.

8.1 Phonebook (Corporate Directory) errors

You can get the following errors on the endpoint if corporate directory is not working properly:

- **Request timed out, no response**
  - The TMS server is busy, try again
- **Warning: directory data not retrieved: 404**
  - The endpoint is configured with the IP address of a different web server than the TMS server
  - The corporate directory path on the endpoint is wrong
- **Warning: directory data not retrieved: 401**
  - The "Public" virtual directory on the TMS server is NOT configured to allow Anonymous Access
- **TMS: No phonebook(s) set on this system**
  - No phonebook(s) set on this system in TMS. Configure the endpoint to subscribe to phonebooks in TMS.
  - Using NAT on the endpoint can lead to TMS not recognizing the system and will not allow it to retrieve any phone books.
- **Request timed out, no response**
  - The endpoint is configured with the IP address of a non existing web server
- **No contact with server**
  - The IIS is restarting or in a state where corrupted messages are received

8.2 TMSDatabaseScannerService

8.2.1 What it does:

The TMSDatabaseScannerService scans the network for new systems and checks the status and configuration of existing systems. The Watchdog Scan Interval specifies the delay for how long TMS will wait after completing a scan before it starts a new scan. The scanner will check the connection status, the call status and the system configuration. If a system in unavailable, it will get that status until the next scan or till the endpoint sends a trap to TMS. The scanner will use SNMP broadcast to detect new systems on the network, which can be limited to certain scan ranges in the "SNMP IP Scan Range" field. Multiple scan ranges can be defined here by comma separating the ranges. By setting this value to 127.0.0.1, TMS will not scan for new systems via SNMP broadcast.

The scanner process is a moderate CPU intensive process for the server, and should be tuned according to the need for updated system information in TMS. To scan one system takes from 2 seconds and up to approximately 20 seconds (worst case); which means that scanning 100 systems might take from 3 minutes and up to 30 minutes.

The scanner will read the system connection status and call status on every scan, but will only read the full system configuration in intervals defined in the "Time to wait before systems in database are rescanned (in hours):" field.

8.2.2 Symptoms:

The system information and system status in TMS is outdated.
Systems not responding still have the status 'InCall' or 'Idle'.

8.2.3 How to fix:

Look in the logs for symptoms or error messages (Logs are found in c:\Program Files\TANDBERG\TMS\wwwTMS\Data\Logs\tmsdebug\log-TMSDatabaseScanner.txt on the server.)
Restarting the service or the TMS server will normally fix any problem with this service.

8.3 TMSLiveService

8.3.1 What it does:

This service allocates conferences on the MCUs, issues the dial commands to the endpoints and the MCUs, and monitors the activity of the participants during a conference.

8.3.2 Symptoms:

The call does not start, and the log in Conference Control Center is almost empty.
You typically only have a line that says "Created" in the log. You might have more lines there if the conference has been changed – but none of them is related to launching the conference

8.3.3 How to fix:

Look in the logs for symptoms or error messages (Logs are found in c:\Program Files\TANDBERG\TMS\wwwTMS\Data\Logs\tmsdebug\log-liveservice.txt on the server.)
Restarting the service or the TMS server will normally fix any problem with this service.

8.4 TMSPLCMDirectoryService

8.4.1 What it does:

This service is responsible for posting phonebooks to Polycom endpoints. The PLCM endpoint retrieves the phonebook from this service when requested via the remote control (like Corporate Directory in TANDBERG Endpoints)

8.4.2 Symptoms:

You don't get any phonebooks on your Polycom endpoints

8.4.3 How to fix:

Look in the logs for symptoms or error messages (Logs are found in c:\Program Files\TANDBERG\TMS\wwwTMS\Data\Logs\tmsdebug\log-plcmdir.txt on the server.)
Restarting the service or the TMS server will normally fix any problem with this service.

8.5 TMSSchedulerService

8.5.1 What it does:

This service is responsible for launching events at set times. Events like System Restore, System Upgrade and Update Phonebooks. This service will also remind the TMSLiveService to start a conference if needed (TMSLiveService will keep track of all booked conferences, but loose this information if it is restarted).

8.5.2 Symptoms:

Scheduled events do not start

8.5.3 How to fix:

Look in the logs for symptoms or error messages (Logs are found in c:\Program Files\TANDBERG\TMS\wwwTMS\Data\Logs\tmsdebug\log-schedulerservice.txt on the server.)
Restarting the service or the TMS server will normally fix any problem with this service.

8.6 TMSSnmpService – TMSWatchdogServiceStarter.exe

8.6.1 What it does:

This service is collecting traps from the endpoints and is putting them directly into the database. It is also responsible for broadcasting SNMP messages to discover newly added systems (the sub ranges for where TMSWatchdogServiceStarter should search for new endpoints can be specified in TMS administrative Tools).

8.6.2 Symptoms:

The statistics are empty.
TMS does not receive system events.
New systems are not automatically discovered.

8.6.3 How to fix:

Make sure no other SNMP tool is running on the server (like HP Openview or other server/network monitoring tools using Microsoft Windows' SNMP Component)
Look in the logs for symptoms or error messages (Logs are found in c:\Program Files\TANDBERG\TMS\wwwTMS\Data\Logs\tmsdebug\log-watchdog.txt on the server.)
Restarting the service or the TMS server will normally fix any problem with this service.

8.7 TMSServerDiagnosticsService

8.7.1 What it does:

This service is responsible for checking the server disk space, the database size and that the other services are running. A TMS ticket is opened if a service is not running, free disk space is less than 10% or the database is 90% of max size.

8.7.2 Symptoms:

Tickets are not opened if service is not running, free disk space is less than 10% or the database is larger than 90% of its max size.

8.7.3 How to fix:

Look in the logs for symptoms or error messages (Logs are found in c:\Program Files\TANDBERG\TMS\wwwTMS\Data\Logs\tmsdebug\log-TMSServerDiagnosticsService.txt on the server.)
Restarting the service or the TMS server will normally fix any problem with this service.

8.8 TMS Database Management Service (optional)

8.8.1 What it does:

This service is installed by the TMS backup utility, and is responsible for doing scheduled backups.

8.8.2 Symptoms:

If the database is not automatically backed up when scheduled, check that this service is installed and is running.

8.8.3 How to fix:

Start up the TMS Database Management Utility and verify the settings in the Automatic Backup page. Checking the "Enable automatic backup" checkbox should normally install the service automatically.

8.9 The Web server

8.9.1 What it does:

TMS is utilizing Microsoft Internet Information Services for making TMS available as a webpage. Since version 9.0 TMS has been developed with the Microsoft .net platform and some extra components are therefore required on the IIS for TMS to work properly. ASP.net version 2.0 was used from TMS 11.5. These components are installed by Windows during the TMS installation as they are required by TMS, but not being TANDBERG specific. All the web-related files will be stored on the server where you specified during the installation; default location is "c:\Program Files\TANDBERG\TMS\"

In the Internet Information Server Manager you will see that the installation has created five virtual directories:

- tms
  - The Application that handles the TMS web interface.
  - The virtual directory for this component on the IIS is: http://serverIP/tms
  - This component should have the Directory Security set to Windows Integrated Authentication (default), Basic Authentication or both

- tms/public
  - Handles Corporate Directory for TANDBERG endpoints
  - Handles http traps from TANDBERG MXP and MPS systems.
  - The virtual directory for this component on the IIS is: http://serverIP/tms/public
  - This component should have the Directory Security set to Anonymous Access

- pwx
  - Handles http traps from Polycom systems
  - Handles phonebooks for Polycom systems
  - The virtual directory for this component on the IIS is: http://serverIP/pwx
  - This component should have the Directory Security set to Anonymous Access
  - This component can be removed if this TMS installation will not be used with Polycom endpoints.

- XAPSite
  - Handles communicator between TMS and pre version 7 MGCs
  - The virtual directory for this component on the IIS is: http://serverIP/XAPSite
  - This component should have the Directory Security set to Anonymous Access
  - This component can be removed if this TMS installation will not be used with a Polycom MGC with version 6.x or older.

- TMSConferenceAPI
  - This component is there to give a warning to the old Exchange API (TMS 7 and 8) that it must be upgraded, and can therefore be removed if the TMS 8 Exchange API is not present in your environment.
  - The virtual directory for this component on the IIS is: http://serverIP/TMSConferenceAPI
  - This component should have the Directory Security set to Anonymous Access
  - This component can be removed if this TMS installation does not have an older Exchange integration (pre TMS 9).

8.9.2 Symptoms:

- You cannot access the TMS page.
- The corporate directory on the TANDBERG endpoints does not work and statistics from TANDBERG MXP endpoints are empty.
- Statistics from Polycom endpoints are empty

8.9.3 How to fix:

- Check that IIS is running
- Check that you can access the default webpage (http://TMSServerName)
- Check that the virtual directories above exists on the TMS server
- Check that they are pointing to valid directories on the TMS server
- Check that the permission settings are correct according to the list above
- Check that the IIS server allows for running .net extensions (ref installation manual)
- Logs are found in c:\Program Files\TANDBERG\TMS\wwwTMS\Data\Logs\tmsdebug\log-web.txt on the TMS server

8.10 Java Applet – Monitoring

8.10.1   What it does:

The Sun Java Applet (Version 1.5.0 (build 1.5.0_06-b05) or newer) is used for displaying dynamic information in Conference Control Center, Graphical Monitor and Map Monitor. The Java Applet gives a lot more functionality for the users when it comes to graphics, clicking, right-clicking and drag-and-drop functions compared to what HTML does.

8.10.2   Symptoms:

1. When entering Conference Control Center, Graphical Monitor or Map Monitor you are prompted for a username and password.
2. The Applet does not load, and there is no Java (Coffee cup) icon in the notification area
3. The Applet does not load, but Java is installed.
4. The Applet loads very slowly
5. Conference snapshots are not displayed on some clients

8.10.3   How to fix:

1. The Java Applet will require the users to authenticate themselves if the TMS server is not part of the domain (or a trusted domain) the user is logged into. The solution is to make the TMS server part of the domain, or insert the username and password when prompted for it (once per session).
2. The Java virtual machine is not installed on the machine, and the client PC does not have direct access to the Internet to download it automatically. Click the question mark icon and click the Java link under the Monitoring main help folder to download the client directly from the TMS server. The link is: http://<<tmsserver>>/TMS/Data/JavaSource/jre-1_5_0_06-windows-i586-p.exe
3. There might be a proxy server hindering the Java Applet to retrieve the necessary data from the TMS server. By opening the Java Console (right click the java icon in the notification area and choose 'Open Console') you will many error messages stating 'unknown source'. To solve this problem please try one or more of the points below:
   o If using the TMS server's IP address when accessing TMS, please try again with the TMS server's host name.
   o Configure the Java client (through the Java Control Panel) to use Direct Connection rather than to use the browser's proxy settings
   o The proxy server may have to be configured to allow this kind of traffic from the TMS server to the clients.

4. The Applet should normally be finished loading within 5 seconds after the Monitoring link is pressed. If you experience a significantly higher loading time, please try the point below:

   o Turn off Caching in Java and delete the existing temporary files.
     (Open the *Java Control Panel*, click the *General* tab, click *Settings*, click *View Applets*, uncheck the *Enable Caching* checkbox in the lower left corner, click *Ok*, click *Delete Files*, check all checkboxes, click *Ok*, click *Ok*, click *Ok)*

   o Remove old or duplicate Java clients from Internet Explorer.
     (Click *Tools* in the Internet Explorer menu, click the *Programs* tab, click *Manage Add-ons* – then disable all old or duplicate java plug-ins)

   o Remove Google Desktop. We have seen issues where Google Desktop is conflicting with the Java plug-in – and significantly increasing the loading time of Java applets. Other desktop search engines like MSN Search does not show the same symptoms.

5. Turn off Caching in Java and/or delete the existing temporary files.
   (Open the *Java Control Panel*, Click the *General* tab, click *Settings*, click *View Applets*, uncheck the *Enable Caching* checkbox in the lower left corner, click *Ok*, click *Delete Files*, check all checkboxes, click *Ok*, click *Ok*, click *Ok)*

8.11 The database

8.11.1   What it does:

The database is where all information about TMS is stored (except software files for system upgrade and the services' log files). The database is called tmsng and can run on SQL 2000 and SQL 2005 servers. During the installation of TMS the sa account on the SQL server is automatically chosen to create and access the database, but a different account can be specified by choosing the 'custom' installation. The account used to run and upgrade TMS must have db_owner permissions to the tmsng database, while a user that also have access to master.mdf is required for creating the tmsng database the first time.

8.11.2   Symptoms:

- TMS does not load and/or you get a 'Stack-trace' describing that the SQL server is unavailable: 'SQL Server does not exist or access denied'

8.11.3   How to fix:

- Make sure that the SQL server is running. This can be done by checking the SQL agent of the server, or going into services and verify that the MSSQLSERVER service is running.
- Run an osql script towards the database as see if it returns any data. This script will return the number of systems in the TMS database:
  - One of these commands should work when running it from the TMS server itself, depending on the SQL configuration.
    - osql -E -d tmsng -Q "select count(*) from objsystem"
    - osql -E -S .\SQLTMS -d tmsng -Q "select count(*) from objsystem"
- Verify that the information TMS uses to connect to the database is correct. This information was historically only stored in the registry, but is from TMS 11.5 also stored encrypted in the web.config file. It is therefore recommended to use the *TMS Tools* application, found under TANDBERG in the Start Menu of the TMS server, to change and verify this information.
- For pre TMS 11.5 verify that the registry key's data field is pointing to the correct server with the correct username. The string value is found in the registry under **My computer\HKEY_LOCAL_MACHINE\SOFTWARE\Tandberg\TANDBERG Management Suite** and is called **tmsngDB**
  - It will look something like this:
    server=(local);database=tmsng;uid=sa;pwd=6D1E89ECEA897E0C4227A DD9DDED93A70143B2FE10517B39DC901352;Connect Timeout=15
    - The **server** value is specifying the IP-address or hostname of the server where the database is
    - The **database** value specifies the name of the database, it can be changed, but problems during upgrade is likely to occur
    - The **uid** value specifies the user used for connecting to the database (must be database owner)
    - The **pwd** value is the password diffused. It can be swapped with a clear text password by changing the name from pwd= to pwd-clear=
      - o easily change the username and password use the TMS tool on the TMS server (in TMS 9.6 or newer)

- The **Connect Timeout** allows you to increase the timeout value for the SQL server to respond to queries. You might want to increase this value if you get SQL timeout error messages on some of the reporting pages in TMS.