

TANDBERG Management Suite and Security

TANDBERG

D13325, rev. 03

Table of contents

TANDBERG Management Suite and Security	1
Table of contents.....	2
Introduction	3
Traffic Load	3
Ports used	3
SNMP Network Policy	4
Authentication – Access control.....	4
External Endpoints	4
Internet Information Server.....	4
Exchange Integration.....	5

Introduction

TANDBERG Managements Suite (TMS) is a tool for monitoring, maintaining and booking video conference systems through a web page. Installing such a service can and often will raise some questions from IT administrators on how this will affect the network in terms of security and performance. This document is meant to address the issues that might come up during an integration of TMS in a company's network.

Traffic Load

A common question is how much traffic or load TMS will put onto a network. TMS is based on a polling system rather than a constant connection model. This means rather than maintaining open connections to devices, TMS will only connect to a device to execute a task or complete a query and then disconnect. In other words, the traffic generated by TMS on the network is a function of how active your systems and users are.

TMS will communicate with devices based on:

Triggers: SNMP Traps generated by the devices based on activity

Events: Timed events like scheduled calls or scheduled maintenance

Timers: Standard polling interval (User defined)

User Interaction: A user requesting new status or refresh from a device

As the protocols used by TMS are relatively lightweight (SNMP, Telnet, HTTP, FTP), even frequent communication has little impact on the network. For example, a SNMP Query packet is on average about 100 bytes. A full connection query in response to a TANDBERG endpoint connecting a call, including all SNMP and Telnet traffic is only approximately 8KB in total. The total impact on your network will depend on the types of devices used, their level of activity, and the level of user interaction on TMS.

Ports used

The following gives an overview of ports used for communication between TMS and videoconference endpoints:

For basic management of video conferencing entities (collecting data, setting parameters, etc):

- TCP port 80 for http
- TCP port 23 for Telnet (and Telnet-Challenge)
- UDP port 161 for SNMP queries
- UDP port 162 for SNMP traps

For software upgrade, phone book settings, company logos, etc:

- TCP port 21 for ftp
- TCP port 20 for ftp data

For end user authentication:

- UDP port 137 and 138 for NetBIOS
- TCP port 57 for Telnet-Challenge

For encrypted communication

- TCP port 443 for https

For automatic detection of new systems

- SNMP broadcast

SNMP Network Policy

TMS relies on SNMP for discovery of and for interaction with devices. It is mandatory that TMS is able to issue SNMP queries to devices. TMS also relies on SNMP Traps from devices to act as triggers to stimulate TMS actions. Often network policies restrict or block SNMP traffic as a security measure. The network security model must allow TMS traffic to devices as well as SNMP Traps from devices, for TMS to operate properly. TMS also uses SNMP Broadcast packets to discover new systems. Often broadcast packets of this type are filtered. If broadcast packets are not allowed, TMS will not be able to automatically discover new systems, but you will still be able to add systems to TMS either through manually entering the address (IP address or DNS name) or by searching an IP address range.

Authentication – Access control

TMS uses the underlying Windows Authentication for logging into TMS. This requires all users have a valid Windows account with access to the TMS server. These accounts could be domain or Active Directory accounts that the server has trust relationship with, or local accounts on the server itself. Once logged on TMS offers a separate permissions model which allows you to group and control users to assign the privileges you desire; all the way from ‘no access’ to ‘site administrator’. Default permissions can also be set, so users can log into TMS and create accounts with no TMS administrator intervention required.

All TANDBERG codecs, gateways, and bridges use the same method of security. When changing the password from the factory default the system requires a strict alphanumeric password with at least 8 characters to be entered. The web browser uses http-digest to authenticate (RFC-2617) and not send the password in clear-text over the IP network. TMS uses MD5-Challenge Response algorithm (RFC-1321) telnet access and also does not send the password in clear-text over the IP network. The only time the password is sent in the clear on the IP network is if a technician uses a client that does not support MD5. Using your internal data network increases the access security of the videoconference devices to the level of other applications running on the network even without using MD5 with telnet.

All TANDBERG equipment ships with internal 56bit DES encryption of the media and all systems support an optional internal 128bit AES encryption. Both encryption algorithms are certified by NIST (the National Institute of Standards and Technology) in February 2003 (DES Certificate #211 and AES Certificate #57 - <http://csrc.nist.gov/cryptval/aes/aesval.html>).

External Endpoints

TMS is constructed for controlling and managing system within a LAN, which means that we recommend using VPN if it is necessary to control and monitor systems outside the company’s physical LAN. If a VPN solution is not possible, the firewall will need to be open on the ports mentioned earlier, for every external VC unit’s IP-address.

Internet Information Server

TMS uses the Microsoft Internet Information Server (IIS) as its web server. The default installation of IIS requires updates from Microsoft and configuration changes to be considered secure. Most IT departments have a configuration policy about IIS; however changes may hinder the functionality required by TMS. TANDBERG supplies a document (Secure Server and IIS for TMS) which can guide you on securing IIS and your server by outlining which security changes are compatible with TMS’s needs.

As always, a firewall blocking unnecessary and unrequested traffic to your servers is recommended.

Exchange Integration

Installing the TMS Exchange Integration does not change the security model of the Exchange or domain environment. During the installation, the administrator is prompted to create three security groups. These groups will be used to administer the permissions for the resource accounts that will be created, and the Active Directory Container to store all the accounts and groups within. Two users will also be created; one is created on the Exchange Server as part of the built-in Administrator group with a strong password to execute the services under, and a normal user is created on the TMS server itself.

TANDBERG Integration Tool is a program that lets an administrator easily create a video conference system on the Exchange server based on the necessary information provided from the TMS server. It also lets administrators update passwords on these accounts if your company's security policy requires it.

The TMS Exchange Integration supports upgrade from Microsoft Exchange server 2000 to Microsoft Exchange server 2003.