

# **Telnet Manager**

---

## **User Guide**

---

## ***Disclaimer***

Honeywell International Inc. ("HII") reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult HII to determine whether any such changes have been made. The information in this publication does not represent a commitment on the part of HII.

HII shall not be liable for technical or editorial errors or omissions contained herein; nor for incidental or consequential damages resulting from the furnishing, performance, or use of this material.

This document contains proprietary information that is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of HII.

© 2004-2017 Honeywell International Inc. All rights reserved.

Web Address: [www.honeywellaidc.com](http://www.honeywellaidc.com)

Microsoft<sup>®</sup>, Windows<sup>®</sup>, Windows Server<sup>®</sup>, and the Windows logo are registered trademarks or trademarks of Microsoft Corporation.

Intel<sup>®</sup> and Intel XScale<sup>®</sup> are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Other product names or marks mentioned in this document may be trademarks or registered trademarks of other companies and are the property of their respective owners.

## ***Patents***

For patent information, please refer to [www.hsmpats.com](http://www.hsmpats.com).

---



# Table of Contents

## **Chapter 1 - Customer Support**

Product Service and Repair .....	1
Technical Assistance .....	1
Limited Warranty .....	1

## **Chapter 2 - Introduction**

About This Manual .....	3
Supported Devices.....	3
Supported Devices.....	3
Features.....	3
SSH Overview.....	4
System Overview .....	4
Telnet Manager .....	4
Quick Start .....	5
DOS Terminal Emulation and Telnet Manager .....	5
RFTerm and Telnet Manager.....	5
Components of a Radio Frequency (RF) System .....	7
Access Points.....	7
Client Devices .....	7
Host.....	7
Wireless Gateway .....	7
Single Network Topology .....	7
Split Network Topology .....	7
Network and System Diagnostics .....	9
Logging .....	9
Telnet Manager for ANSI, IBM 3270, IBM 5250.....	9
Alarms .....	9
Diagnostics.....	9
Telnet Manager Capabilities for ANSI, IBM 3270 and IBM 5250 .....	9
Identifying Mobile Computers .....	11
ANSI.....	11
IBM 3270 / TN3270, IBM 5250 / TN5250.....	11
Important Information for Upgrading TM1 Software Load.....	11

## **Chapter 3 - Telnet Manager Installation and Operation**

System Requirements.....	13
Installation Errors .....	13
Uninstall Earlier Version Warning .....	13
.NET Framework Error.....	13
Installation.....	13
Ports and Firewalls .....	19
Ports.....	19
Firewalls.....	19
Windows XP SP2/SP3 and Windows Server 2003 .....	19
All Other Firewalls .....	20

---

SSH Setup.....	20
Part 1: Windows Setup .....	20
Part 2: WinSSHD Setup.....	20
Part 3: Host Computer Setup.....	22
WinSSHD Defaults .....	22
Uninstall or Repair Installation.....	23
SSH Uninstall.....	23
Uninstalling a Previous Version .....	23
Stop Telnet Manager Scheduled Task .....	24
Reboot Before Installation .....	24
Using Add or Remove Programs .....	24
Using Telnet Manager CD .....	24
Preserved Files.....	26
Registry Entries .....	26
Log Files .....	26
Utilities .....	27
TM1Reg.....	27
Save.....	27
Restore .....	28
Delete .....	28
Demo Mode .....	28
Launching Telnet Manager.....	29
TM1Config Configuration Utility .....	29
TM1 Service.....	29
Starting/Restarting TM1 Service.....	30
Stopping TM1 Service .....	31
TM1Console .....	31
Commands .....	32
? .....	32
sList .....	32
sDump index.....	32
sIAC index .....	34
sClose index .....	34
sAllClose.....	34
sSetDBLevel x .....	34
resetLog.....	35
version .....	35
quit .....	35
stopService.....	35
Configuration Utility Interface .....	35
Components .....	35
Browser Panel .....	36
Browser Panel Color Schemes.....	37
Icons .....	37

## **Chapter 4 - ANSI Configuration Utility**

Introduction.....	39
-------------------	----

---

ANSI Telnet Manager Components.....	39
Global Configuration.....	39
Client Registration.....	39
Client Registration Master Template Parameters.....	39
Client Registration Registered Client Parameters.....	40
AutoLogin Script.....	40
Master Autologin Parameters.....	40
Individual Autologin Parameters.....	40
Registration License.....	40
ANSI Global Configuration Parameters.....	40
Factory Defaults.....	40
Buttons.....	40
Restore Values to Factory Default.....	40
Save current values.....	41
Restart Service.....	41
Parameters.....	41
Terminal Connection.....	41
Terminal ID Mode.....	41
Radio Server Fast Failover.....	42
TCP/IP Host KeepAlive.....	42
Connection Response Delay.....	43
SNMP Traps.....	43
Log File.....	44
Dialog / Error Boxes.....	44
Directory Does Not Exist.....	44
Logfile Directory Error.....	45
Parameter Change Notification.....	45
Global Configuration Save.....	46
ANSI Client Registration.....	46
Registering New Client Devices.....	47
Factory Defaults.....	47
Buttons.....	47
Parameters.....	47
Client Registration / Master Template.....	48
Factory Defaults.....	49
Buttons.....	49
Parameters.....	49
Dialog / Error Boxes.....	52
Client Registration / Registered Clients.....	52
Factory Defaults.....	54
Buttons.....	54
Parameters.....	54
Dialog / Error Boxes.....	57
ANSI AutoLogin Scripts.....	58
Creating New AutoLogin Scripts.....	58
Buttons.....	59
Parameters.....	59

---

Dialog Boxes / Errors.....	59
AutoLogin Scripts / Master Template.....	60
Factory Defaults.....	62
Buttons.....	62
Parameters .....	62
Dialog Boxes / Errors.....	63
AutoLogin Scripts / Named Scripts .....	64
Buttons.....	64
Parameters .....	65
Dialog Boxes / Errors.....	66
Removing a Named AutoLogin Script.....	67
License Registration .....	67
Buttons.....	68
Submit.....	68
Restart Service .....	68

### **Chapter 5 - IBM 3270 Configuration Utility**

Introduction.....	69
IBM 3270 Telnet Manager Components.....	69
Global Configuration .....	69
Client Registration .....	69
Client Registration Master Template Parameters.....	69
Client Registration Registered Client Parameters .....	70
Registration License .....	70
IBM 3270 Global Configuration Parameters.....	70
Factory Defaults.....	70
Buttons.....	70
Restore Values to Factory Default.....	70
Save current values .....	70
Restart Service .....	70
Parameters .....	71
Terminal Connection.....	71
Terminal ID Mode .....	71
Radio Server Fast Failover .....	71
TCP/IP Host KeepAlive.....	71
Connection Response Delay .....	72
SNMP Traps .....	72
Log File .....	73
Dialog / Error Boxes.....	73
Directory Does Not Exist.....	73
Logfile Directory Error .....	74
Parameter Change Notification.....	74
Global Configuration Save .....	75
IBM 3270 Client Registration.....	75
Registering New Client Devices .....	76
Factory Defaults.....	76
Buttons.....	76

---

Parameters .....	76
Client Registration / Master Template .....	77
Factory Defaults.....	78
Buttons.....	78
Parameters .....	78
Dialog / Error Boxes.....	80
Client Registration / Registered Clients .....	81
Factory Defaults.....	82
Buttons.....	82
Parameters .....	83
Dialog / Error Boxes.....	85
License Registration .....	86
Buttons.....	87
Submit.....	87
Restart Service .....	87

## **Chapter 6 - IBM 5250 Configuration Utility**

Introduction .....	89
IBM 5250 Telnet Manager Components.....	89
Global Configuration .....	89
Client Registration .....	89
Client Registration Master Template Parameters.....	89
Client Registration Registered Client Parameters .....	90
Registration License .....	90
IBM 5250 Global Configuration Parameters.....	90
Factory Defaults.....	90
Buttons.....	90
Restore Values to Factory Default .....	90
Save current values .....	90
Restart Service .....	90
Parameters .....	91
Terminal Connection.....	91
Terminal ID Mode .....	91
Radio Server Fast Failover .....	91
TCP/IP Host KeepAlive.....	91
Connection Response Delay .....	92
SNMP Traps .....	92
Log File .....	93
Dialog / Error Boxes.....	94
Directory Does Not Exist.....	94
Logfile Directory Error .....	94
Parameter Change Notification.....	94
Global Configuration Save .....	95
IBM 5250 Client Registration.....	95
Registering New Client Devices .....	96
Factory Defaults.....	96
Buttons.....	96

---

Parameters .....	96
Client Registration / Master Template .....	97
Factory Defaults.....	98
Buttons.....	98
Parameters .....	98
Dialog / Error Boxes.....	100
Client Registration / Registered Clients .....	101
Factory Defaults.....	102
Buttons.....	102
Parameters .....	103
Dialog / Error Boxes.....	105
License Registration .....	106
Buttons.....	107
Submit.....	107
Restart Service .....	107

## **Chapter 7 - SSH Settings**

Introduction .....	109
Select Profile .....	109
Select Profile List.....	109
Create New Profile.....	109
Profile Name .....	109
Save Profile .....	110
SSH Server.....	110
Address.....	110
Port .....	110
Authorization.....	110
User+Pswd .....	110
User .....	110
Password .....	110
Key File.....	110
User .....	110
Passphrase.....	110
User Key File .....	110
Allow connection to unlisted host.....	110
Advanced Settings.....	111
Keep Alive Ping Interval.....	111
Rekey After MB of Data .....	111
Rekey After Minutes .....	111
Compression.....	111
Server Keys .....	111
Global Allowed Host Keys .....	111
Delete .....	111
PuTTY Key Generator .....	111
Public Key.....	113
Private Key .....	113



---

## **Chapter 8 - Logs, SNMP Traps and Reference Material**

Telnet Manager Log Files.....	115
Windows Event Log.....	115
Debug Log.....	116
Example Debug Log File.....	116
SNMP Traps.....	117
LXE MIB SNMP Trapping.....	118
Decimal – Hexadecimal Equivalents.....	119

## **Chapter 9 - SSH: Telnet Manager and RFTerm Case Study**

Introduction.....	121
Example Configuration.....	121
Microsoft Windows User Account and Firewall Configuration.....	121
Step 1: User Account.....	121
Step 2: Open Port.....	121
WinSSHD-LXETM1 Setup.....	121
Step 1: WinSSDH Settings.....	122
Step 2: Save User Info.....	122
Step 3: Edit Settings.....	122
Step 4: Create Virtual Account.....	122
Step 5: Configure Virtual Account.....	122
Step 6: Save.....	123
Step 7: Export.....	123
Step 8: Start WinSSHD.....	123
Host Computer Setup.....	123
Telnet Manager Configuration.....	124
Step 1: Global Configuration.....	124
Step 2: Restart Service.....	124
Step 3: Master Template.....	124
Step 4: Create Profile.....	124
Step 5: Save.....	125
Step 6: AutoLogin Scripts.....	125
RFTerm Configuration.....	125
Step 1: Start RFTerm.....	125
Step 2: Configure Session.....	125
Step 3: Configure SSH.....	125
Step 4: User Authorization.....	126
Step 5: AutoLogin.....	126
Step 6: Close Configuration.....	126
Step 7: Data Processing.....	126
Other Examples.....	127
SSH for RFTerm to Telnet Manager Only.....	127
SSH for Telnet Manager to Host Only.....	127
SSH Help.....	127



## *Customer Support*

### ***Product Service and Repair***

Honeywell International Inc. provides service for all of its products through service centers throughout the world. To obtain warranty or non-warranty service, please visit [www.honeywellaidc.com](http://www.honeywellaidc.com) and select **Support > Contact Service and Repair** to see your region's instructions on how to obtain a Return Material Authorization number (RMA #). You should do this prior to returning the product.

### ***Technical Assistance***

If you need assistance installing or troubleshooting your device, please contact us by using one of the methods below:

**Knowledge Base:** [www.hsmknowledgebase.com](http://www.hsmknowledgebase.com)

Our Knowledge Base provides thousands of immediate solutions. If the Knowledge Base cannot help, our Technical Support Portal (see below) provides an easy way to report your problem or ask your question.

**Technical Support Portal:** [www.hsmsupportportal.com](http://www.hsmsupportportal.com)

The Technical Support Portal not only allows you to report your problem, but it also provides immediate solutions to your technical issues by searching our Knowledge Base. With the Portal, you can submit and track your questions online and send and receive attachments.

**Web form:** [www.hsmcontactsupport.com](http://www.hsmcontactsupport.com)

You can contact our technical support team directly by filling out our online support form. Enter your contact details and the description of the question/problem.

**Telephone:** [www.honeywellaidc.com/locations](http://www.honeywellaidc.com/locations)

For our latest contact information, please check our website at the link above.

### ***Limited Warranty***

Refer to [www.honeywellaidc.com/warranty\\_information](http://www.honeywellaidc.com/warranty_information) for your product's warranty information.



## About This Manual

This manual is intended for users of the Telnet Manager software product.  
The TM1 Telnet Manager Appliance (hardware) product is obsolete.

## Supported Devices

Telnet Manager is for use with computers running Honeywell RFTerm™. The following devices support RFTerm:

## Supported Devices

The following devices support RFTerm:

- MX7 Tecton (Windows CE 6.0, Windows Mobile 6.5)
- Thor VM1 (Windows CE 6.0, Windows Embedded Standard 2009)
- Thor VM2 (Windows CE 6.0, Windows Embedded Standard 2009, Windows 7, Windows Embedded Standard 7)
- Thor VX8 and Thor VX9 (Windows XP, Windows 7, Windows Embedded Standard 2009)

*Note: RFTerm may be supported on other devices not listed, including obsolete devices.*

## Features

Telnet Manager features:

- ANSI session management support for up to 500 wireless/wired radio devices
- IBM 3270 session management support for up to 500 wireless/wired radio devices
- IBM 5250 session management support for up to 500 wireless/wired radio devices
- Installs on user supplied Telnet Manager Server; a PC with Microsoft® .NET Framework 1.1 installed and Windows® XP Professional SP2/SP3, Windows® 7 (32-bit or 64-bit), Windows Server® 2008 (32-bit or 64-bit), or Windows Server® 2003 SP1 operating system.

*Note: An upgrade to Telnet Manager may be required for Windows 7 support. Contact [Technical Assistance](#) (page 1) for information.*



The Telnet Manager can support up to 500 mobile devices per server without any performance issues. If the mobile device number exceeds 500, there is a possibility of deteriorated performance or loss of features

A client device running a Telnet-based terminal emulation connects via the RF network through an Access Point (AP) to the Local Area Network (LAN). The client is then connected to the Telnet Manager Server which relays the connection to the host. Telnet Manager, being an intermediary, provides the following functionality:

- Session Maintenance – maintains initial session with host while the client is “absent,” that is, out-of-range or powered down.
- Terminal Keep Alive – Monitors the client connection during periods of no traffic, terminates the client device session with the host if the operator fails to respond to Telnet Manager polls.
- Activity Timeout – actively terminates the client device session with the host if the client does not use the computer for a given time.
- Autologin – automatic login of the client device without the active intervention of the user, login timeouts if the client device does not respond in a timely manner.
- Configuration – display active client devices, set Autologin script, save setup, etc.
- Support for SSH Shell connections (ANSI only) and SSH tunnel connections (ANSI, IBM 3250 and IBM 5250).



Some implementations of SSH in Telnet Manager used Bitwise Tunnelier. Contact [Technical Assistance](#) (page 1) for the archived version of this document if using a version of Telnet Manager that includes Tunnelier.

---

## SSH Overview

Telnet Manager supports SSH v2 via the use of WinSSHD. This program is installed when the Include SSH checkbox is selected during Telnet Manager installation.

Bitwise WinSSHD is an SSH Secure Shell 2 server. WinSSHD runs as a service and is automatically started. The instance of the WinSSHD server installed for Telnet Manager is named "WinSSHD-LXETM1". Because WinSSHD communicates special information about the terminals to the Telnet Manager, it is required to use WinSSHD and not any other SSH server. You may configure WinSSHD to use a non-standard port to avoid conflict with an existing SSH server.

When RFTerm (running on a mobile computer) is configured to use SSH, it makes an encrypted connection to the Telnet Manager's WinSSHD server. WinSSHD decrypts the data and forwards the connection to the Telnet Manager. There is no configuration necessary in the Telnet Manager for this incoming connection. If SSH is enabled on the Client Registration Master Template, the default SSH tunnel is created at TM1 startup. This eliminates a possible delay as it can take up to 20 seconds to establish an SSH tunnel when the first terminal tries to connect. Any unregistered terminal connection uses the Master Template.

Whether or not SSH is enabled on the Master Template, individual registered terminals may customize their connection to the host so they can be directed to connect via a normal telnet connection or by a separate SSH connection.

If SSH is not enabled on the Master Template or any terminal clients specify a custom SSH profile (differing from the Master Template), the SSH tunnel is not established until the terminal connects for the first time which may result in a delay of up to 20 seconds as the SSH tunnel is established.

SSH tunnels are not closed when the client disconnects. They are closed only when the TM1 service is stopped.

For more information, refer to:

- [SSH Setup](#) (page 20) in Telnet Manager Installation and Operation.
- Client Registration/Master Template and Client Registration/Registered Clients in the appropriate installed emulation: [ANSI Configuration Utility](#) (page 39), [IBM 3270 Configuration Utility](#) (page 69) or [IBM 5250 Configuration Utility](#) (page 89).

## System Overview

Honeywell's Telnet Manager provides host session management for TCP/IP RF data collection systems. It is designed to stabilize the performance of an RF network comprising RF connected computers (client devices), an RF backbone and a host computer.

Telnet Manager is designed to compensate for the unreliable nature of the wireless connections; unexpected, intermittent breaks in RF coverage and/or unexpected momentary downtime of battery-powered wireless devices. Telnet Manager requires Microsoft Windows XP Professional Service Pack 2 or greater, Windows 7, Windows Server 2003 Service Pack 1 or greater, or Windows Server 2008.

Telnet Manager offers several installation options. Only one option may be installed at a given time:

- Telnet Manager for ANSI
- Telnet Manager for IBM 3270
- Telnet Manager for IBM 5250

### **Telnet Manager**

Telnet Manager includes support for ANSI, IBM 3270 or IBM 5250 emulations with an option for Secure Shell (SSH) connections between the Host and the Telnet Manager as well as between the Telnet Manager and the client devices (mobile computers).

Telnet Manager consists of a Configuration Utility (TM1Config), a Windows service (LXE TM1) and a Console Application (TM1Console). The TM1 service runs in the background. A command line interface is provided by the Console Application. Additionally, to support SSH, additional components are installed if the Include SSH option is selected during TM1 installation.

Telnet Manager installs in demo mode. The demo is valid for 30 days from the date of installation. A Registration Key is necessary to license Telnet Manager and continue use beyond the demo period. The license key is entered in the Configuration Utility. Refer to the appropriate area for more information on the TM1Config utility and the license key:

- [ANSI Configuration Utility](#) (page 39)
- [IBM 3270 Configuration Utility](#) (page 69)

- [IBM 5250 Configuration Utility](#) (page 89)

## Quick Start

These instructions are abbreviated and give a general outline of the steps to be performed when setting up a new Telnet Manager system. Details may be found in the links referenced in each step.

1. Connect the Telnet Manager Server to the Ethernet backbone(s).
2. Install Telnet Manager on the Telnet Manager Server. See [Telnet Manager Installation and Operation](#) (page 13).
3. If SSH support is enabled, configure [SSH Setup](#) (page 20).
4. Edit connection parameters for Telnet Manager using TM1Config:
  - [ANSI Configuration Utility](#) (page 39)
  - [IBM 3270 Configuration Utility](#) (page 69)
  - [IBM 5250 Configuration Utility](#) (page 89)
5. Start [TM1 Service](#) (page 29).

Client devices must have access to the Ethernet network before they can communicate with the Telnet Manager Server. The Access Point provides that access. This document assumes the client devices are properly configured to connect to a wireless backbone that provides access to the Ethernet network.

## DOS Terminal Emulation and Telnet Manager

DOS equipped client devices (ANSI Plus, Plus, TN3270 or TN5250) must be configured properly to be used with Telnet Manager. The following field values must be set in the client devices:

Client Device Parameter	ANSI Plus	TN3270	TN5250
Autologin	Enabled	Disabled	Disabled
Prompt / Reply	Blank	N/A	N/A
Host	IP Address of Telnet Manager		
Port	As set in Telnet Manager, see <b>Note 1</b>		
Enable2ndID	See <b>Note 2</b>	N/A	N/A
SecondaryID	See <b>Note 2</b>	N/A	N/A

### Note 1:

The Port value must match the one of the Port settings in the TM1Config using the Client Registration screens. Default values are 400, 4001, 4002 and 4003.

### Note 2:

**Use Secondary ID/Enable2ndID** and **Secondary ID** must be enabled if Telnet Manager Terminal ID mode is set to Secondary ID. An entry is required for the **Secondary ID/SecondaryID** field. Otherwise, **Use Secondary ID/Enable2ndID** should be Disabled and the **Secondary ID** is not applicable.

## RFTerm and Telnet Manager

Microsoft Windows equipped client devices (using RFTerm™) must be configured properly to be used with Telnet Manager. The following field values must be set in the client devices: For an example of using RFTerm with Telnet Manager, see [SSH: Telnet Manager and RFTerm Case Study](#) (page 121).

Client Device Parameter	ANSI	IBM 3270	IBM 5250
Autologin	Enabled	Disabled	Disabled
Prompt / Reply	Blank	N/A	N/A

---

Client Device Parameter	ANSI	IBM 3270	IBM 5250
Host	IP Address of Telnet Manager		
Port	As set in Telnet Manager, see <b>Note 1</b>		
Use Secondary ID	See <b>Note 2</b>	N/A	N/A
Secondary ID	See <b>Note 2</b>	N/A	N/A
SSH Server Address	IP Address for WinSSHD, see <b>Note 3</b>		

**Note 1:**

The **Port** value must match the one of the Port settings in the TM1Config using the Client Registration screens. Default values are 400, 4001, 4002 and 4003.

**Note 2:**

**Use Secondary ID/Enable2ndID** and **Secondary ID** must be enabled if Telnet Manager Terminal ID mode is set to Secondary ID. An entry is required for the **Secondary ID/SecondaryID** field. Otherwise, **Use Secondary ID/Enable2ndID** should be Disabled and the Secondary ID is not applicable.

**Note 3:**

The SSH Server must be specified if using Secure Shell connections. **SSH Select** must be set to either *Shell* or *Tunnel* in RFTerm. Specify the IP address of the WinSSHD server here. This is the same IP address as the Telnet Manager.



---

## Components of a Radio Frequency (RF) System

### Access Points

Access Points (AP) are hardware and software products that perform an Ethernet to Radio Frequency (RF) bridging function over radios in the 2.4GHz band. The AP is the bridge between wireless client devices and the Telnet Manager Server. The AP is typically connected to the wired Ethernet backbone and is stationary.

### Client Devices

Client devices (for the purpose of this manual) are hardware and software products that connect to Access Points over radios in the 2.4GHz band in the Telnet Manager system. Client devices are lightweight, sturdy, seldom stationary and sometimes mounted on vehicles. Some client devices are powered by replaceable batteries, while others accept power from the vehicle battery. These client devices are designed to be easily moved from place to place while maintaining a wireless connection to the wireless components of the Telnet Manager system.

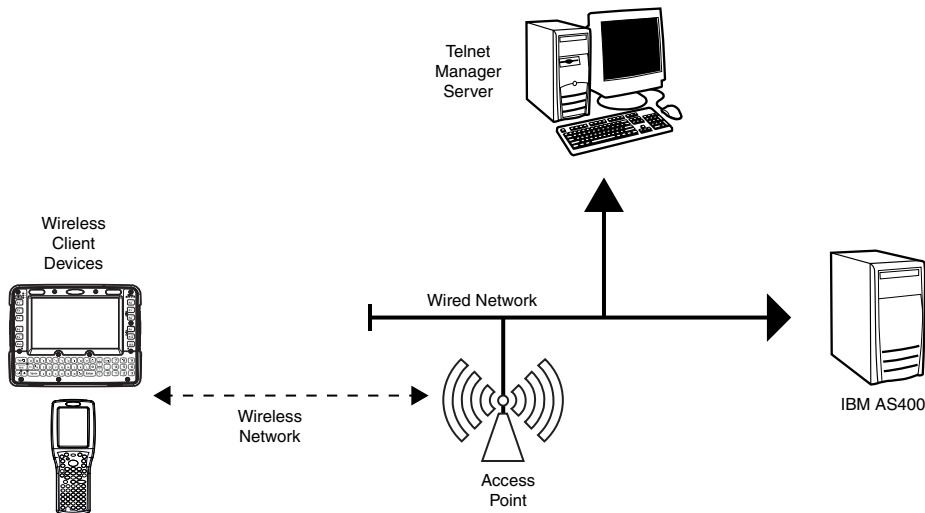
### Host

A computer that runs application programs and maintains databases.

## Wireless Gateway

### Single Network Topology

Typically, the Telnet Manager Server connects to the Ethernet backbone through a single network interface. This situation is diagrammed below. In it, all Ethernet traffic to and from the Telnet Manager Server and the wireless access points is visible to any other device on the network. Conversely, all devices on the Ethernet segment are also visible to all the wireless devices.



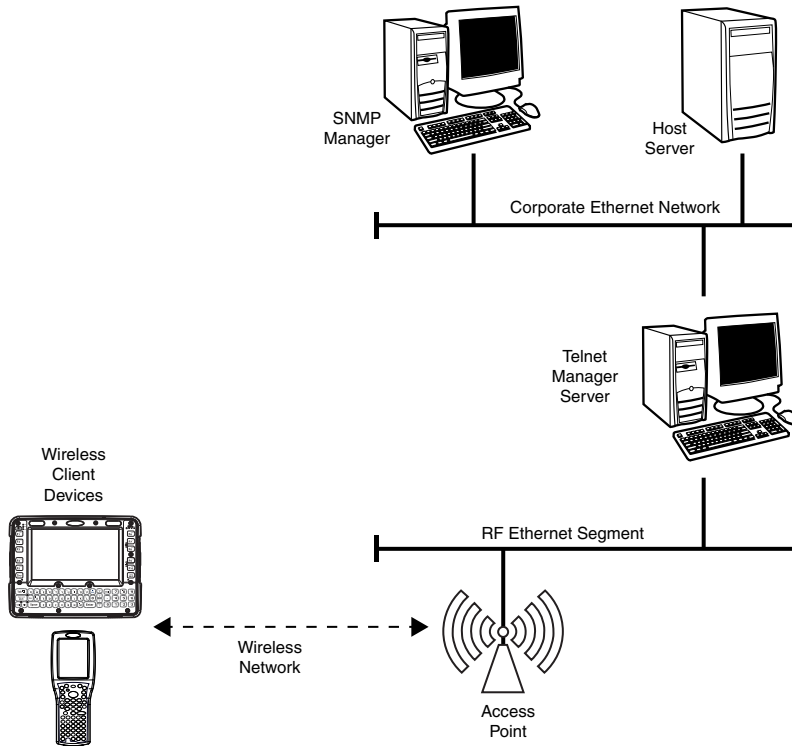
While this is typically how data collection networks are designed today, it does pose some security risk, as an attacker with a modest amount of 802.11b enabled computing equipment may be able to get access to the corporate network.

The topology above also allows an SNMP manager (not shown) to optionally receive traps from Telnet Manager and to convert those traps into appropriate messages to the network administrator.

### Split Network Topology

As an alternative, the Telnet Manager Server may be configured to act as a router device between the wireless data collection network and the corporate network. In this case, the Telnet Manager Server has at least two Ethernet interfaces. By configuring one Ethernet interface to handle host traffic and the other Ethernet interface to handle traffic to the client devices, the Telnet Manager Server can effectively act as a router between the two backbones.

The Telnet Manager can pass traffic from the wireless network interface only to specific configured IP addresses on the host side interface. Likewise, only traffic from those configured IP addresses on the host network interface is passed to the wireless interface.



This functionality is offered as an additional access security feature for those enterprises concerned with the vulnerability of their wireless networks. It limits the type of traffic an eavesdropper has access to on the wireless network, and it limits the accessibility of an intruder to the corporate network. Note, however, that this is not expected to be a bulletproof security measure.

Telnet Manager runs on Windows XP, Windows 7, Windows Server 2003 or Windows Server 2008. From time to time, security vulnerabilities in these operating systems are identified and sometimes exploited. The Telnet Manager application does not attempt to enhance any of the security components of the Windows operating system. Any operating system may have security flaws that would allow an intruder to bypass the Telnet Manager. Telnet Manager software will, at best, present another roadblock to a would-be intruder.

Optionally, the topology above also allows an SNMP manager to be located on the corporate network side of the Telnet Manager units. The SNMP manager is to receive traps from Telnet Manager and to convert those traps into appropriate messages to the network administrator.

---

## **Network and System Diagnostics**

Three types of diagnostics are available at the Telnet Manager Server.

### **Logging**

#### ***Telnet Manager for ANSI, IBM 3270, IBM 5250***

Telnet Manager has two logging functions.

Telnet Manager writes entries into the Event Viewer log. The log can be viewed by selecting **Start > Control Panel > Administrative Tools**. Click on Application to open the log. The Telnet Manager entries are denoted by LXE TM1 in the Source column. Additionally, installation entries may be present for the Telnet Manager installer denoted by Msiln-staller in the Source column.

Telnet Manager also creates an optional debug log file. The location of this file is specified via the TM1Config utility. The debug level can be set via the registry (none, high detail, intermediate detail, low detail).

The logging may be disabled or the log files may be limited in number and size via the Global Configuration parameters. See "Global Configuration" in the sections linked below.

See Also

[IBM 3270 Configuration Utility](#) (page 69)

[IBM 5250 Configuration Utility](#) (page 89)

[Telnet Manager Log Files](#) (page 115)

### **Alarms**

Optionally, Telnet Manager can generate alarms (which are SNMP Traps) for:

- Application host communications failure. An alarm event Trap is generated if Telnet Manager loses communications with any host for which a session is currently open.
- Terminal communications failure. Telnet Manager generates an alarm event if a specific client device is disconnected due to a 'keep-alive' time out or user activity time out.
- Telnet Manager Reset. When Telnet Manager goes through a Boot or Reset for whatever reason a "Cold StartTrap" is generated.

See Also

[SNMP Traps](#) (page 117)

### **Diagnostics**

The system diagnostic parameters include:

- List of current active sessions.
- The ability to terminate any single session.
- The ability to terminate all sessions.
- The ability to set the Debug level.
- The ability to reset the Log file
- The ability to examine the IAC exchange between the client and host.

See Also

[Debug Log](#) (page 116)

## **Telnet Manager Capabilities for ANSI, IBM 3270 and IBM 5250**

Telnet Manager provides the capability to manage the individual sessions between the mobile clients and the host computer.

---

Telnet Manager acts as a proxy for the actual client devices from the application host perspective. The Telnet Manager Server is cabled to the physically connected network and has a reliable connection to the application host. The application host addresses all RF traffic to Telnet Manager, allowing the application host to function in a manner oblivious to the wireless devices.

<b>Feature</b>	<b>Description</b>
Telnet Session Keep-Alive	The 'keep-alive' functionality of Telnet Manager maintains the host session connection during intervals when the actual client device is not responding to network traffic.
Reconnect After Power Cycle	At times, the client device may be powered off without having logged out of the host application session. This may happen, for example, if the user shuts the computer down to change batteries. Upon power up the user can reconnect to the same session.
TE Inactivity Timer	The ability to log the user off of the host application if there has been no client activity for a specified time period.
Terminal Autologin	This function essentially duplicates the autologin function found on the client device (ANSI only).
Session Management Across Router Boundaries	Client sessions can be managed regardless of where the mobile device is located on the network.
Host Autologin Script Management	The user can create host autologin scripts that can be shared across multiple client devices (ANSI only).
Terminal DHCP	Client devices can now enable DHCP since the device can be managed by the RF MAC address.
Secure Shell	Terminals can connect via telnet, SSH tunnel connection or SSH Shell connection (ANSI only).

Telnet Manager runs as a Windows service.

---

## ***Identifying Mobile Computers***

By default, Telnet Manager uses the MAC address of the mobile computer radio to identify the device. The MAC address is used to guarantee consistent identification in case a site is using dynamic IP addressing. The MAC address for a radio remains constant and properly identifies the mobile device in all environments. When using MAC address as the mobile computer identifier, the devices are properly identified unless the radio module in the device is changed.

To provide compatibility with installations using previous products, alternate methods of mobile computer identification are provided.

### ***ANSI***

For sites that use legacy DOS ANSI Plus terminal emulation or RFTerm's ANSI emulation, the ENQ response can be used to identify the mobile computer. See the Secondary ID option for [Terminal ID Mode](#) (page 41) for details on using the ENQ response to identify computers.

### ***IBM 3270 / TN3270, IBM 5250 / TN5250***

For sites that use one of the legacy DOS IBM terminal emulations (either TN3270 or TN5250) or RFTerm's IBM 3270 or IBM 5250 emulations, the mobile computer IP address can be used as the identifier. See the IP Address option for Terminal ID Mode (IBM3270: [Terminal ID Mode](#) (page 71); IBM 5250: [Terminal ID Mode](#) (page 91)) for details on using the IP address to identify computers.

Also note that this method, like the legacy 6224 Session Manager, does not reliably support clients configured to use DHCP since the IP address may change.

## ***Important Information for Upgrading TM1 Software Load***

The Telnet Manager software product can be used to upgrade the software loaded on the TM1 Telnet Manager Appliance. Some of the features described in this guide may differ. Refer to the Telnet Manager Appliance Reference Guide for details.



## Telnet Manager Installation and Operation

### System Requirements

Telnet Manager can be installed on the customer's hardware. The PC, referred to in this manual as the Telnet Manager Server, must meet the following requirements:

- Intel Celeron 563MHz CPU or greater, minimum 256MB RAM,
- Display set to 96 dpi,
- Microsoft .NET Framework 2.0 or greater must be installed (Earlier versions of Telnet Manager required .NET Framework 1.1 or greater.)
- Operating system must be Windows XP Professional SP2 or greater, Windows 7, Windows Server 2003 SP1 or greater, or Windows Server 2008. Telnet Manager has been tested and validated on systems running Microsoft Windows XP Professional Service Pack 2/Service Pack 3, Windows 7 (32-bit and 64-bit), the 32-bit version of Microsoft Windows Server 2003 SP1 Standard Edition and Windows Server 2008 (32-bit and 64-bit). Telnet Manager does not support Windows XP 64-bit, or Windows Vista operating systems.

Telnet Manager software can also be installed on the TM1 appliance to update the appliance's current software installation. If this option is selected, refer to the installation instructions found here as well as the "Telnet Manager Appliance Reference Guide" for information specific to the TM1 hardware platform. Contact [Technical Assistance](#) (page 1) for more information.

### Installation Errors

If an error message appears when trying to install Telnet Manager, review the sections below to resolve the error before installation.

#### Uninstall Earlier Version Warning

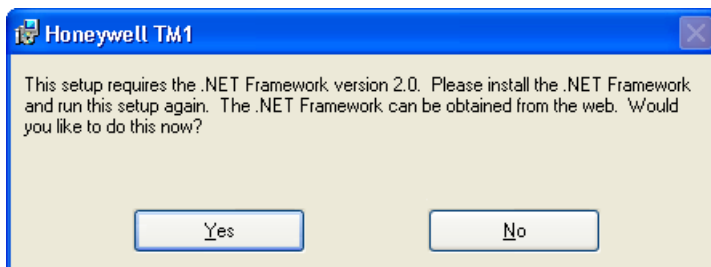
Some versions of the Telnet Manager require the uninstallation of a previous version before the new version can be installed.



Refer to [Uninstall or Repair Installation](#) (page 23) for details. It is necessary to follow the instructions for a successful uninstallation.

#### .NET Framework Error

Telnet Manager requires Microsoft .NET Framework 2.0 or greater (earlier versions of Telnet Manager could run on 1.1 or greater). If the .NET Framework 2.0 is not installed, it must be installed before the Telnet Manager software. An error message is displayed during Telnet Manager installation if the .NET framework is not installed or is an older version.



- Clicking the Yes button directs you to Microsoft's download site and exits the installation process.
- Clicking the No button exits the installation process.

Once the .NET Framework is installed, restart the Telnet Manager installation process.

*Note: Microsoft's .NET Framework 2.0 SP1 is also included on the Telnet Manager CD ROM and may be installed from the CD.*

### Installation

Only one emulation may be selected for installation (i.e.: ANSI Telnet Manager, IBM 3270 Telnet Manager or IBM 5250 Telnet Manager). To install a different emulation it is necessary to first uninstall the old emulation then install the new desired emulation.

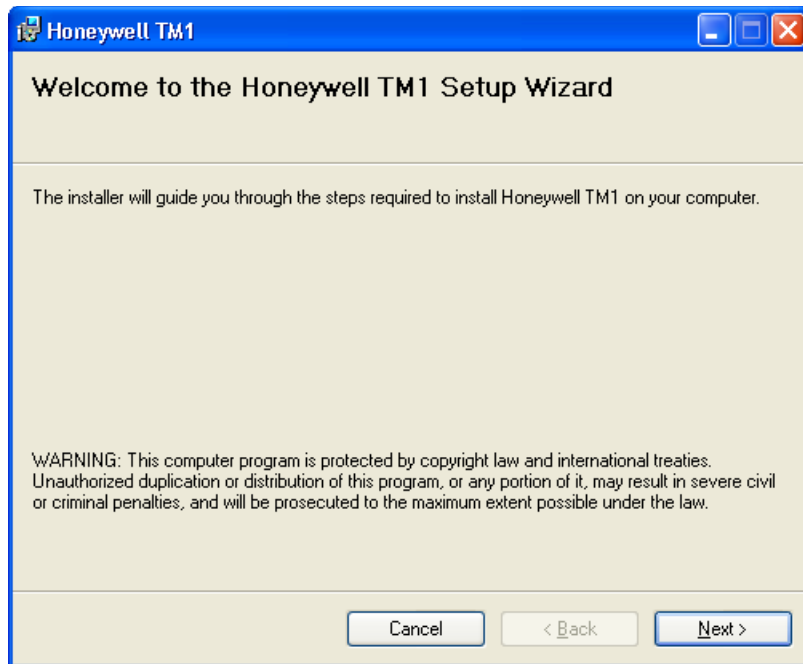
---

Telnet Manager must be installed from a User Account with Administrator privileges.

Insert the Telnet Manager CD-ROM in the CD drive.

Using Windows Explorer, locate the **TM1Setup.msi** file on the CD and double-click on the icon.

The Setup Wizard opens.



*Note: If the Setup Wizard does not open and a .NET Framework warning is displayed, see [.NET Framework Error](#).*

*Note: If the same version of Telnet Manager is already installed, the Repair/Remove screen is displayed. See [Uninstall or Repair Installation](#) (page 23) for details.*

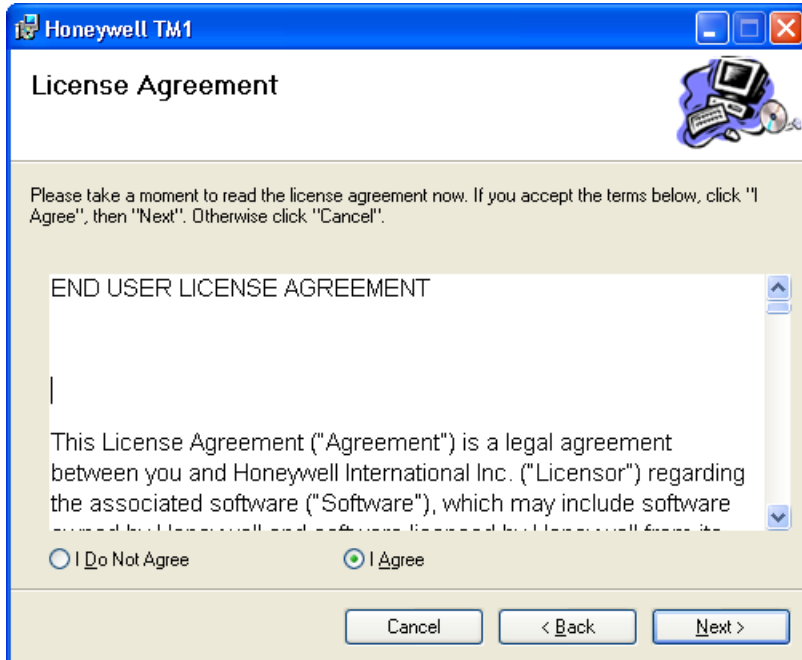
*Note: If a warning message is displayed indicating that “Another version of this product is already installed” see [Uninstall or Repair Installation](#) (page 23) for details.*

To continue the installation process, click the **Next >** button.

Click the Cancel button to exit without installing Telnet Manager.

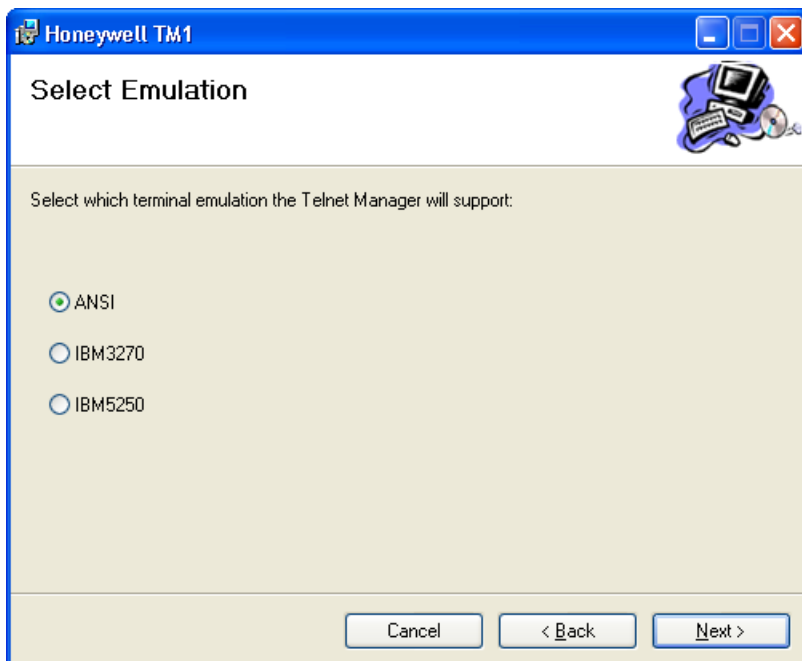
The Software License Agreement is displayed.





Review the software license.

If you agree to the terms, click the **I Agree** radio button then click **Next >**. Otherwise, click the **Cancel** button to exit the installation process.



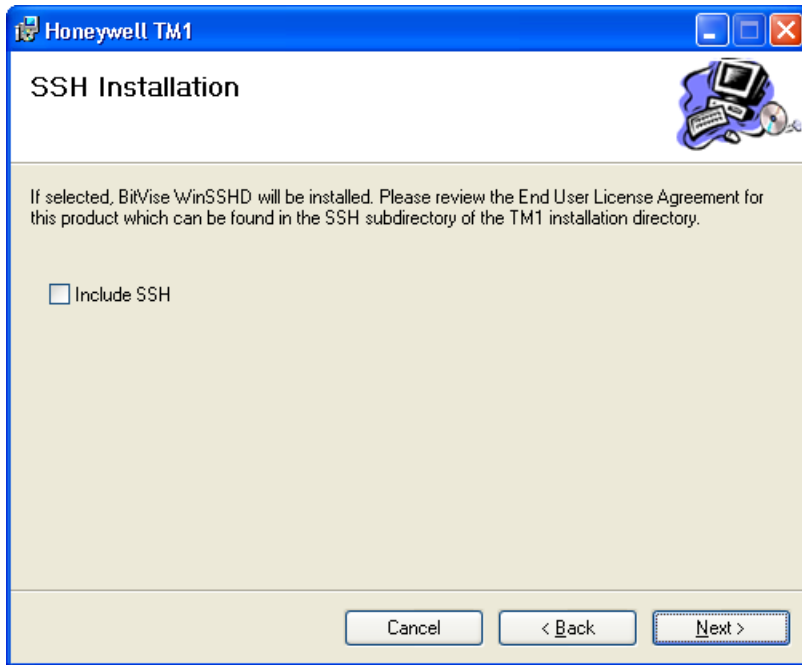
Click on the radio button for the desired terminal emulation and click the **Next >** button.

Click the **< Back** button to return to the previous screen to make changes.

Click the **Cancel** button to exit without installing Telnet Manager.

*Note: Only one Terminal Emulation may be selected. In order to switch Terminal Emulations, Telnet Manager must first be uninstalled then installed with the desired Terminal Emulation selected.*

If SSH is desired, check the **Include SSH** checkbox. If SSH is selected, additional components are installed automatically during the installation process.



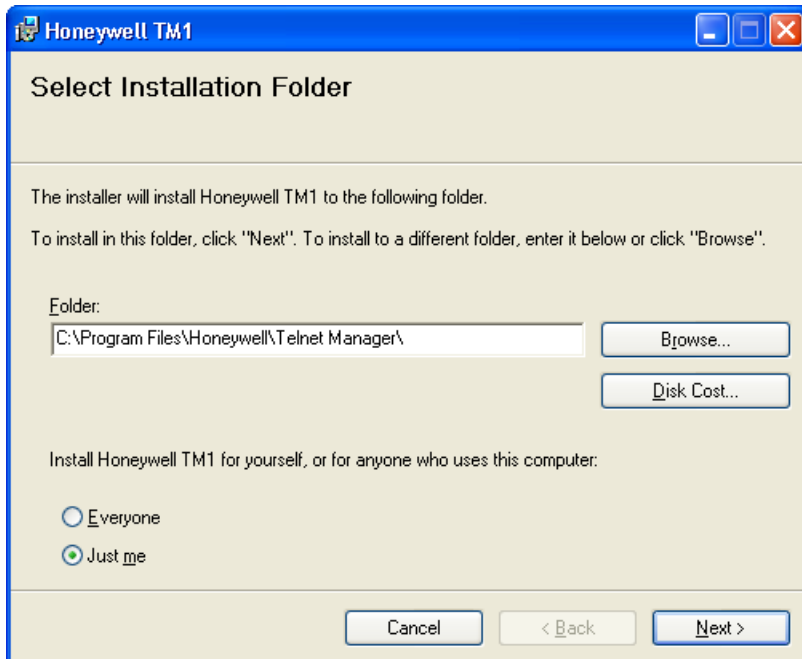
Choose the desired installation options.



If there is an existing installation of Bitvise SSH products (such as if Telnet Manager was uninstalled, but the Bitvise products were not), follow these steps before clicking Next to continue Telnet Manager installation.

- Exit Tunnelier, if present (earlier version of SSH implementation used Tunnelier)
- Close the WinSSHD Control Panel.

If the Bitvise products are not already installed, click **Next >** to continue.



---

Enter the desired installation folder for Telnet Manager. The default is:

- C:\Program Files\Honeywell\Telnet Manager\ (for 32-bit systems)
- C:\Program Files (x86)\Honeywell\Telnet Manager\ (for 64-bit systems).

To select a different installation directory:

- Type in the directory path desired, or
- Use the **Browse...** button to navigate to and select the desired directory

Click the **Disk Cost...** button to see a list of available disk drives and space available on each.

Select the users who have access to Telnet Manager icons:

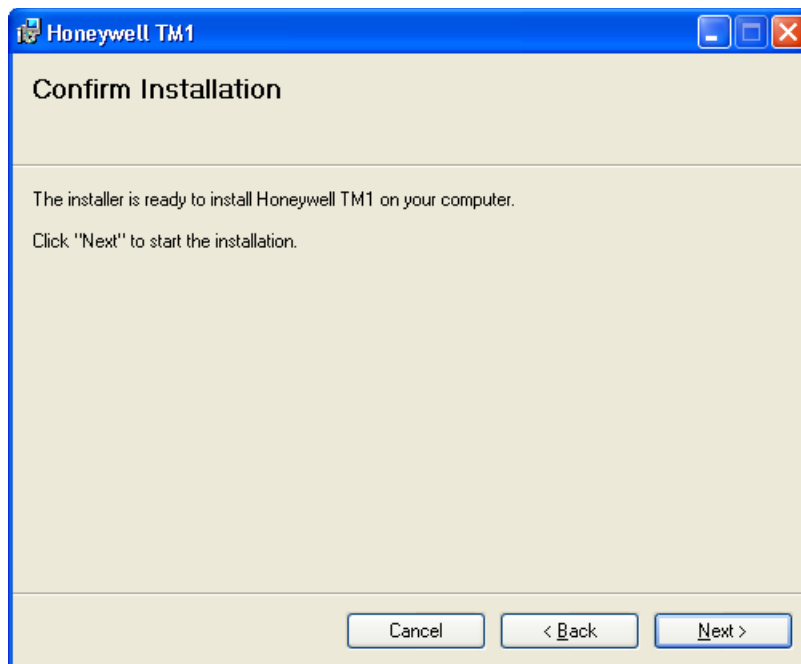
- Click the **Just me** button to restrict the startup icons to the user account installing Telnet Manager. This option is strongly recommended.
- Click the **Everyone** button for all users to have access to Telnet Manager Desktop and Start Menu icons.

*Note: While this installation option determines which users have access to the desktop and start menu icons for Telnet Manager, any user can still launch the TM1Config or TM1Console utilities from the installation directory.*

*Note: A user must have administrative access to run the TM1Config and TM1Console utilities or to start the TM1 service.*

When the desired directory and user access have been selected, click the **Next >** button to continue the installation process.

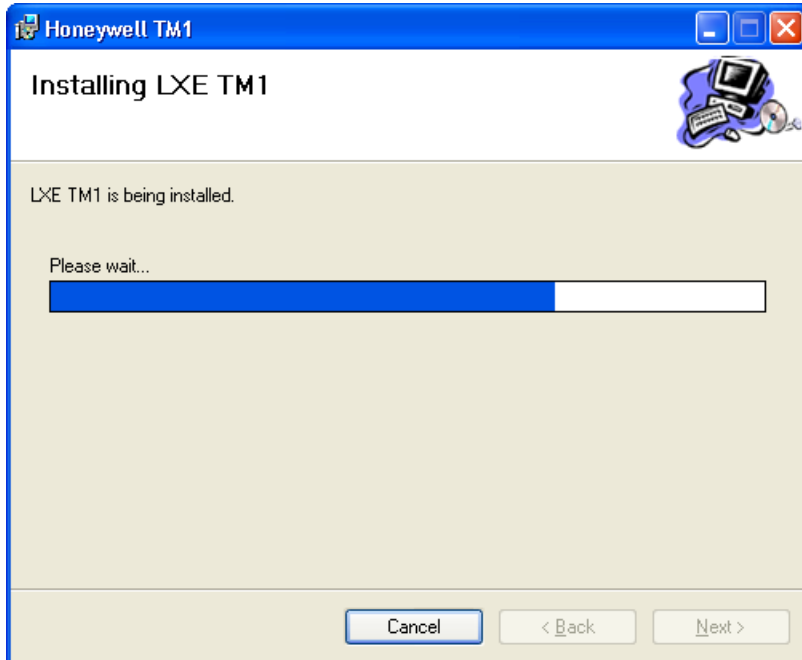
Click the **Cancel** button to exit without installing Telnet Manager.



If you are happy with the installation configuration, click the **Next >** button to begin the installation.

Click the **< Back** button to return to the previous screen to make changes.

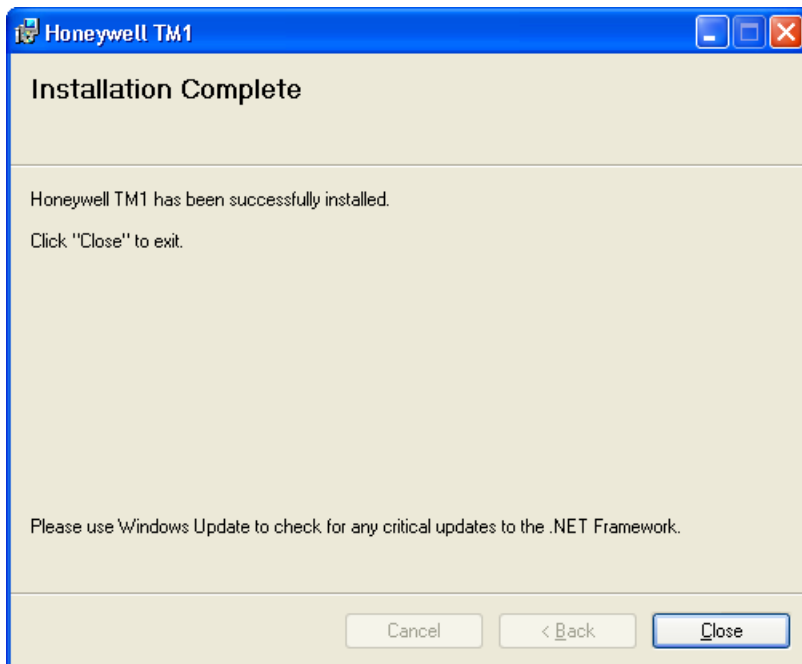
Click the **Cancel** button to exit without installing Telnet Manager.



Click the **Cancel** button to stop the installation. Otherwise, wait until the process is completed.

If the SSH option was selected, Bitvise WinSSHD is automatically installed. There is no visual indication of WinSSHD installation during this process. If SSH was not selected, Bitvise WinSSHD is not installed.

Once the installation is complete, the installation completed screen is displayed.



Click the **Close** button to exit the installation routine.



Be sure to check the Microsoft Windows Update page to ensure all critical updates have been installed. There may be new critical updates, especially if the .NET Framework was recently installed on the computer.

---

Launch the TM1Config utility ([ANSI Configuration Utility](#) (page 39), [IBM 3270 Configuration Utility](#) (page 69) or [IBM 5250 Configuration Utility](#) (page 89)) and access the Global Configuration screen and click the **Save Current Values** button after making any desired changes.

The TM1 service can now be started. The service may be started by clicking the “Restart Service” button on the TM1Config screen or by several other methods. See [Starting/Restarting TM1 Service](#) (page 30) for more details.

*Note: The TM1 service cannot be started until the initial configuration has been performed using TM1Config.*

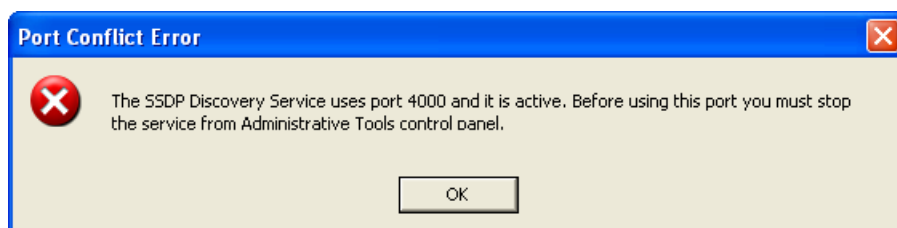
## Ports and Firewalls

### Ports

Telnet Manager uses the following ports for ANSI, IBM 3270 and IBM 5250:

- Terminal Connection Port 1 (default value 4000)
- Terminal Connection Port 2 (default value 4001)
- Terminal Connection Port 3 (default value 4002)
- Terminal Connection Port 4 (default value 4003)
- Fast Failover Message Port (ANSI only, default value 4004)

When TM1Config is launched, the application checks to see if the SSDP Discovery Service is currently running and if it is using the same port as Telnet Manager. If a conflict is discovered, a warning message is displayed.



To eliminate the conflict:

- Use the **Administrative Tools > Services** option in the Microsoft Windows Control panel to stop the conflicting service and free up the port for Telnet Manager. Refer to on-line Windows Help for more information, or
- Change the conflicting port in Telnet Manager to a new port. Refer to the appropriate link for your terminal emulation ([ANSI Configuration Utility](#) (page 39), [IBM 3270 Configuration Utility](#) (page 69) or [IBM 5250 Configuration Utility](#) (page 89)) for information on changing the ports used by Telnet Manager.



After making the desired changes to the ports using TM1Config, click the Save current values button, and then click the Restart service button. It is necessary to restart the TM1 Service after any port changes are made. Restarting the service terminates any existing client connections.

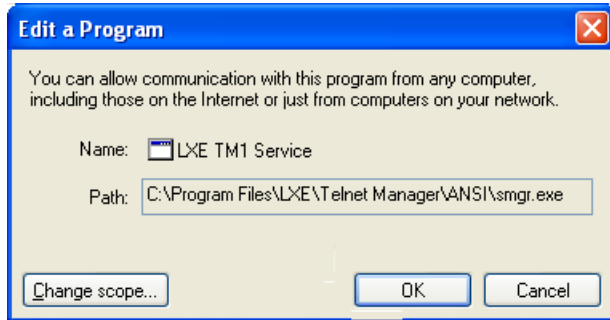
### Firewalls

When Telnet Manager is installed on a computer with a firewall, the firewall must be configured to allow the ports used by Telnet Manager.

#### **Windows XP SP2/SP3 and Windows Server 2003**

When Telnet Manager is installed on a computer running Microsoft Windows XP or Windows Server 2003, the Windows Firewall configuration is modified to accommodate the Telnet Manager program.

The entry made can be viewed by selecting **Start > Control Panel > Windows Firewall**. Click on the Exceptions tab. Find “LXE TM1 Service” and double-click it for more details.



*Note: The firewall ports are opened to all computers on the network, not just computers on the local subnet. Click the Change Scope button to restrict access for greater security if necessary.*

More information on the Windows Firewall can be obtained via the Windows help feature.

### **All Other Firewalls**

For all other firewalls, the third party firewall must be manually configured to:

- Open the ports listed in “Ports”. If any change is made to the ports listed on the TM1Config configuration screen, be sure to update the firewall to reflect those changes, – or –
- Provide access so that the Telnet Manager program automatically has access to whatever ports it needs

## **SSH Setup**

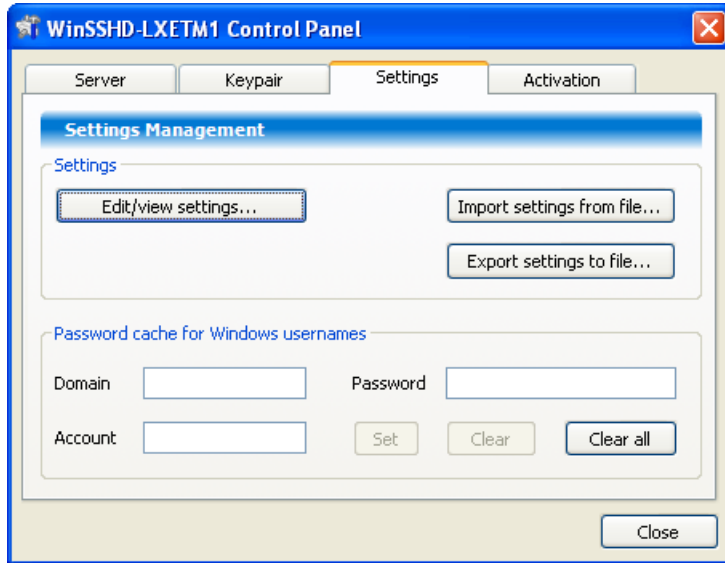
The setup instructions for SSH are detailed in the three parts below.

### **Part 1: Windows Setup**

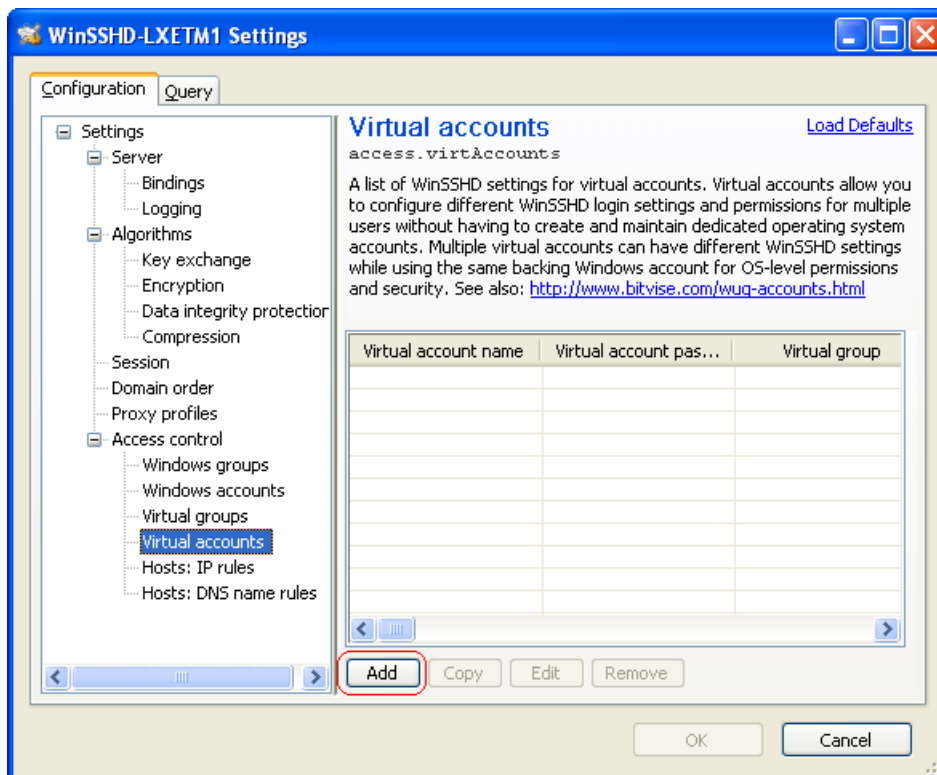
1. Open a port for the WinSSHD-LXETM1 SSH server in the firewall. The default port is 22. See [Part 2: WinSSHD Setup](#) (page 20) for more details.
2. Add a user account for incoming SSH connections. An existing user account may be used if desired. If using an existing account, the password should be set to never expire.
3. Select **Control Panel > Administrative Tools > Computer Management > Local Users and Groups**.
4. Select **Users**. Right click and select **New User....**
5. Enter the desired Username, for example **ssh-server-guest**.
6. Set a password for the user account.
7. Make sure **User must change password at next login** is NOT checked and click **OK**.
8. Double click on the new user entry and select **Password never expires**.
9. It is NOT necessary for this account to have Administrator privileges.

### **Part 2: WinSSHD Setup**

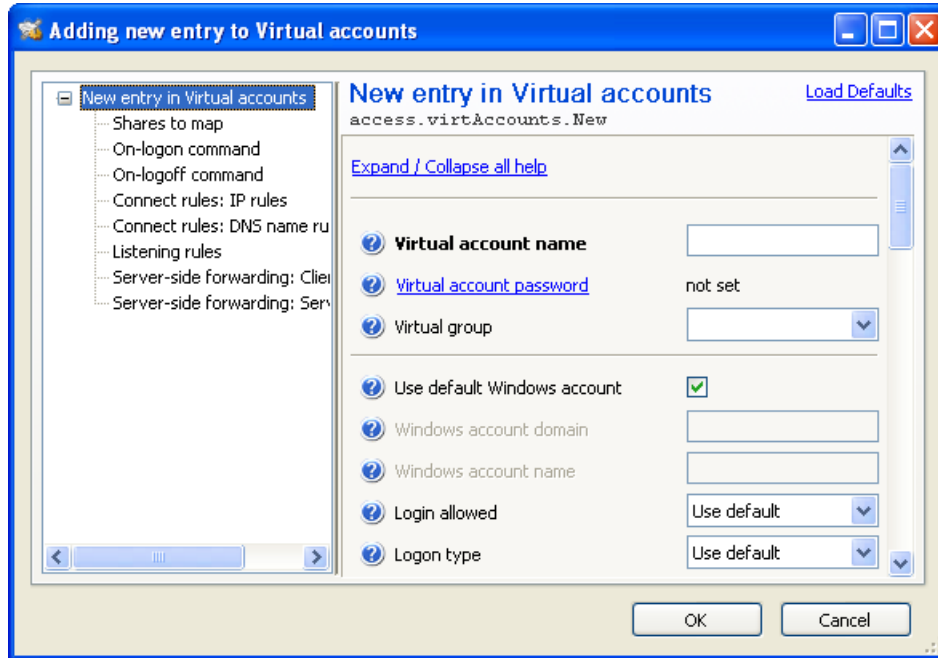
1. Access the WinSSHD control panel by selecting **Start > All Programs > Bitvise WinSSHD-LXETM1 > WinSSHD-LXETM1 Control Panel**.
2. Select the **Settings** tab.



3. In the Password cache for Windows usernames section, enter the following:
  - **Account** – the user account created above, for example ssh-server-guest
  - **Password** – The password assigned when the account was created.
4. Click **Set**.
5. Click the **Edit/view settings...** button.
6. Make sure the **Configuration** tab is selected.



7. Under Access Control, select **Virtual accounts**. Click the **Add** button.



8. Use the following settings:

- **Virtual account name** - (user defined), for example ssh-guest
- **Virtual account password** - (user defined)
- **Virtual group** - Virtual Users
- **Use default Windows account** - False
- **Windows account name** - (user defined), for example ssh-server-guest. Must match the account name for the User Account created in Windows Setup, above.

9. Click **OK**, click **OK**

10. Click **Export settings to file....** Save the file. The file is saved with an extension of **.wst**. This file can be imported at a later time to restore these settings as necessary.

11. Click the **Server** tab. Click the **Start WinSSHD** button. Click **Close**.

### **Part 3: Host Computer Setup**

*Note: Telnet Manager has been tested using WinSSHD as the host SSH server. Other SSH servers may be used.*

1. Set up an SSH server configured to use port 22 (the default port) or other specified ports.
2. Setup an SSH account and record your host SSH username and host SSH password. These do not have to be the same as those set for WinSSHD on the TM1 server.  
If a public/private key is to be used, see [PuTTY Key Generator](#) (page 111) for more information.
3. Check the SSH server's session timeout make it never timeout. On WinSSHD this is done via the WinSSHD Control Panel in **Settings > Session > Session Timeout = 0**.

### **WinSSHD Defaults**

The installation of WinSSHD is in a custom location under the directory chosen for the Telnet Manager (C:\Program Files\Honeywell\Telnet Manager\SSH or ,C:\Program Files (x86)\Honeywell\Telnet Manager\SSH by default). Because it is installed in a unique directory, the installation and configuration of WinSSHD for the Telnet Manager does not affect any other installations of WinSSHD that may already be installed on the PC. The customized copy of WinSSHD is labeled Bit-verse WinSSHD-LXETM1.

Additionally, the Tenet Manager installation makes several changes to the default WinSSHD parameters: From the WinSSHD-LXETM1 control panel:



---

**Settings > Server**

**Accept delay (ms)** is “1”

**Settings > Server > Logging**

**Windows Event Log logging level** is set to “Custom Events”.

**Windows Event Log events** has #261 unchecked.

**Settings > Access control > Windows groups**

**Group type** “everyone”

**Login allowed** – false.

**Settings > Access control > Virtual groups**

**Group type** “Virtual Users”

**Password authentication** – Required

**Permit remote administration** – false

**Permit terminal shell** – false

**Permit exec requests** – false

**Settings > Session**

**Session Timeout** is set to “0” (so a session never times out)

## ***Uninstall or Repair Installation***

The Uninstall or Repair routine can be initiated from the Windows Control Panel or from the Telnet Manager CD.

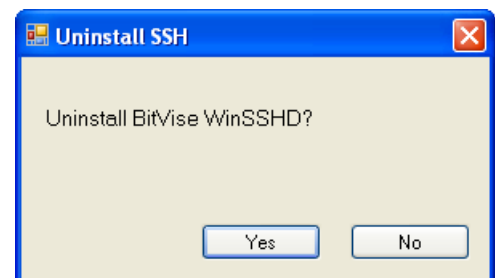
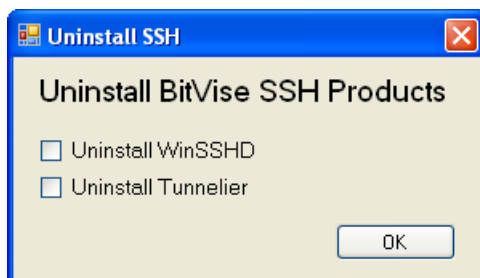
Before uninstalling Telnet Manager or performing a repair installation, be sure to exit any open instances of the TM1Config and TM1Console utilities.

### ***SSH Uninstall***

When uninstalling a version of Telnet Manager that includes SSH support, an option is provided to also uninstall WinSSHD and Tunnelier if desired. Tunnelier is only used for SSH support in some versions of the Telnet Manager

During the uninstall process, select the desired components to remove when prompted and click the OK button. The Uninstall SSH prompt may differ depending on which version of Telnet Manager was installed.

*Note: There is no need to uninstall the SSH components when upgrading Telnet Manager.*



### ***Uninstalling a Previous Version***

If you are currently using version 2 or earlier of Telnet Manager it may be running as a scheduled task. Therefore it is necessary to take additional steps to ensure a successful uninstall of the previous version. Use one of the two methods detailed below:

---

### **Stop Telnet Manager Scheduled Task**

1. Check **Control Panel > Scheduled Tasks** to see if a task named **smgr.exe** is listed. If listed, perform these steps. If it is not listed, then Telnet Manager is running as a service and these steps are not necessary.
2. Prior to uninstalling, use the Windows Task Manager to locate the appropriate Telnet Manager process (smgransi.exe, smgr3270.exe or smgr5250.exe).
3. Select the process, and click the **End Process** button.
4. Proceed with the uninstall process as detailed in “Using Add or Remove Programs”, below.

### **Reboot Before Installation**

1. Using this method, it is not necessary to stop the Scheduled Task.
2. Proceed with the uninstall process as detailed in “Using Add or Remove Programs”, below.
3. Reboot the PC after uninstalling the previous version.
4. After the reboot completes, install the new version.

### **Using Add or Remove Programs**

To use this option, click on the Add or Remove Programs icon and locate LXE TM1 in the program listing.

- Click the Remove button and follow any on screen instructions to uninstall Telnet Manager.
- Clicking the Change button. In this case, the both the Repair Telnet Manager and Remove Telnet Manager options are available. Follow any on screen instructions to complete the selected process.

The uninstall process also removes any registry settings and saves them to the Windows temporary file location. Log files are also preserved after uninstallation. See “Preserved Files” for details.

The repair installation process reinstalls Telnet Manager. This option differs from the initial install because the repair installation procedure does not present any options to the user. Instead, the repair installation uses the same options as the initial installation. Customized Master Templates, Client Registration and Autologin Scripts are not affected by the repair installation.

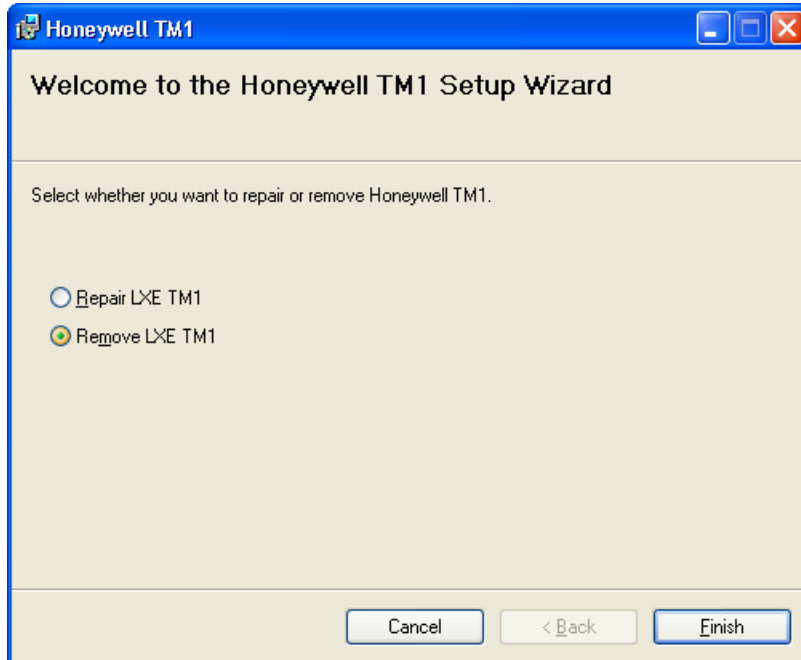
### **Using Telnet Manager CD**

To uninstall or repair Telnet Manager, insert the Telnet Manager CD.

Using Windows Explorer, locate the TM1Setup.msi file on the CD and double-click on the icon.

If Telnet Manager has been previously installed, the following screen is displayed.

*Note: If Telnet Manager is not installed, the Installation screen is displayed.*

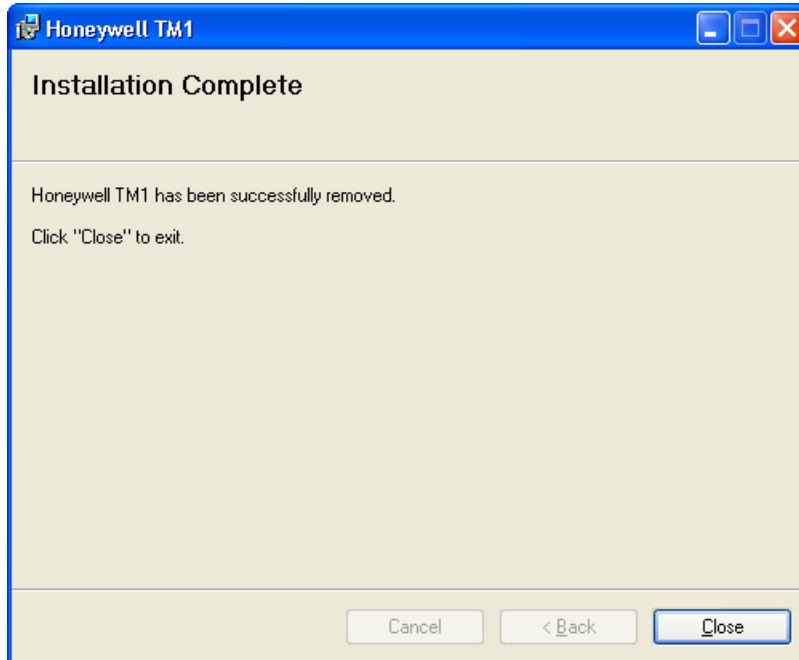


Select **Remove Telnet Manager** and click **Finish** to uninstall Telnet Manager.

Select **Repair Telnet Manager** and click **Finish** to repair the Telnet Manager installation.

Click **Cancel** to exit without uninstalling.

Follow the on screen instructions to uninstall or repair Telnet Manager.



*Note:* Click **Close** to exit.

*Note:* The uninstall process also removes any Telnet Manager registry settings and saves them to the Windows temporary file location. Log files are also preserved after uninstallation. See [Preserved Files](#) (page 26) for details. If the SSH products are uninstalled, their settings are not automatically preserved.

*Note:* The repair installation process reinstalls Telnet Manager. This option differs from the initial install because the repair installation procedure does not present any options to the user. Instead, the repair installation uses the same options as the initial installation. Customized Master Templates, Client Registration and Autologin Scripts are not affected by the repair installation.

## **Preserved Files**

The uninstall process preserves some Telnet Manager files. See the following sections for details.

*Note:* You may wish to view the Global Configuration screen and make a note of the log file location before uninstalling Telnet Manager if the installation directory or log file directory were customized.

The Event Logger entries ([Windows Event Log](#) (page 115)) are preserved after uninstall. However, the Category and Event IDs are not preserved.

### **Registry Entries**

When Telnet Manager is uninstalled, Telnet Manager settings are removed from the registry. They are stored as .REG files in the Windows Temp directory, for example: C:\Documents and Settings\\Local Settings\Temp.

The registry settings are saved in two files:

- tm1Appsave.reg
- tm1SYSsave.reg

When a new version of Telnet Manager is installed, it checks for these saved settings files in the Temp directory and applies them to the new installation.

These files should be removed (or moved to a different location) prior to installing a different emulation instance of Telnet Manager.

- The Windows Temp directory is not intended as permanent storage. If the files are to be preserved, copy or move them a different directory.

### **Log Files**

When Telnet Manager is uninstalled, the log files are preserved.

---

The default location for the log files varies based on the emulation selected:

- C:\Program Files\Honeywell\Telnet Manager\ANSI\log (32-bit system)
- C:\Program Files (X86)\Honeywell\Telnet Manager\ANSI\log (64-bit system)
- C:\Program Files\Honeywell\Telnet Manager\IBM3270\log (32-bit system)
- C:\Program Files (x86)\Honeywell\Telnet Manager\IBM3270\log (64-bit system)
- C:\Program Files\Honeywell\Telnet Manager\IBM5250\log (32-bit system)
- C:\Program Files (x86)\Honeywell\Telnet Manager\IBM5250\log (64-bit system)
- (if SSH installed) C:\Program Files\Honeywell\Telnet Manager\WinSSHD-LXETM1\Logs (32-bit system)
- (if SSH installed) C:\Program Files (x86)\Honeywell\Telnet Manager\WinSSHD-LXETM1\Logs (64-bit system)

If a different installation directory was selected or the log file location was customized on the configuration screen, the log files are located in a different directory.

*Note: The log file location can be determined by viewing the tm1Appsave.reg file mentioned in the previous section.*

## Utilities

Telnet Manager includes a registry utility. By default the utility is located in one of the following directories:

- C:\Program Files\Honeywell\Telnet Manager\TM1Config\bin (32-bit system)
- C:\Program Files (x86)\Honeywell\Telnet Manager\TM1Config\bin (64-bit system)

If Telnet Manager was installed in a custom directory, look in the \Telnet Manager\TM1Config\bin directory off the customized install directory.



The TM1ServiceInstaller located in the \bin folder is used by the install/uninstall process. DO NOT use this utility.

### TM1Reg

The TM1Reg.exe is a command utility used to save, restore or delete Telnet Manager registry keys.

If the TM1Reg utility is called with no parameter, i.e.:

```
TM1Reg
```

Usage instructions are displayed.

```
Usage: TM1Reg save [directory]
       or: TM1Reg restore [directory]
       or: TM1Reg delete
```

where [directory] is the installation directory if unspecified.

### Save

The Save parameter is used to save Telnet Manager registry keys to a pair of .REG files in the specified location.

#### Usage

The usage of the save parameter is:

```
TM1Reg save [directory]
```

Where [directory] is a user specified directory. The directory must already exist as this command does not create the directory. If no directory is specified with the command, the installation directory is used, which is either:

```
C:\Program Files\Honeywell\Telnet Manager
C:\Program Files (x86)\Honeywell\Telnet Manager
```

#### Result

On success, the following messages are displayed:

```
Successful save of HKEY_LOCAL_MACHINE\SOFTWARE\LXE\TelnetManager\.
Successful save of HKEY_LOCAL_MACHINE\SOFTWARE\TM1_LXE_SYSTEM\.
```

If the directory does not exist, an error message is returned:

```
Directory c:\test does not exist.
```

---

## Restore

The Restore parameter is used to restore previously saved Telnet Manager registry keys from .REG files in the specified location. The Restore parameter can also be used with .REG files from a previous uninstall. See [Preserved Files](#) (page 26) for more information.

### Usage

The usage of the restore parameter is:

```
TM1Reg restore [directory]
```

Where [directory] is a user specified directory. The directory must already exist as this command does not create the directory. If no directory is specified with the command, the installation directory is used, which is either:

```
C:\Program Files\Honeywell\Telnet Manager
```

```
C:\Program Files (x86)\Honeywell\Telnet Manager
```

### Result

On success, the following messages are displayed:

```
Successful restore of HKEY_LOCAL_MACHINE\SOFTWARE\LXE\TelnetManager\.
```

```
Successful restore of HKEY_LOCAL_MACHINE\SOFTWARE\TM1_LXE_SYSTEM\.
```

If no registry files are found, an error message is displayed:

```
Registry backup file c:\regtest\tmlAppsave.reg is missing.
```

```
Registry backup file c:\cons\tmlSYSsave.reg is missing.
```

If the directory does not exist, an error message is returned:

```
Directory c:\test does not exist.
```

## Delete

The Delete parameter is used to delete all Telnet Manager keys from the registry.

### Usage

The usage of the delete parameter is:

```
TM1Reg delete
```

### Result

On success, no message is displayed.

If the directory keys were previously deleted, an error message is returned:

```
Cannot delete a subkey tree because the subkey does not exist.
```

This option only deletes the registry key. It does not uninstall Telnet Manager. If the TM1Config utility is launched after the registry keys are deleted, the registry keys are recreated with the default values.

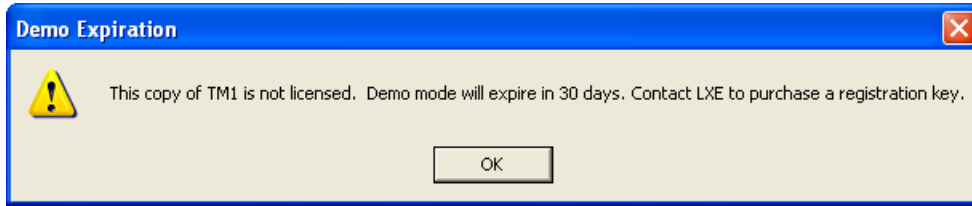
*Note: If the registry keys are deleted, Telnet Manager cannot be launched. If a launch is attempted, errors are encountered and the launch is aborted. Default settings can be restored by launching TM1Config.*



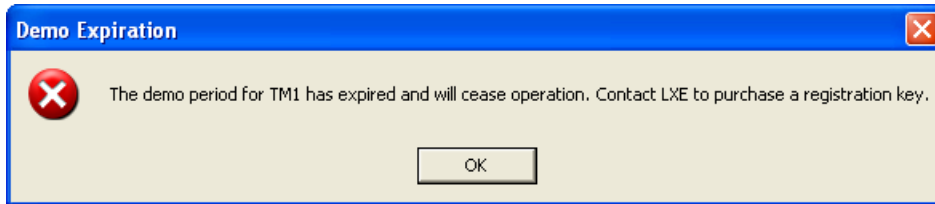
This option is used during the uninstall procedure and should not normally be used manually.

## Demo Mode

By default, Telnet Manager is installed in Demo mode. The Demo is valid for 30 days from the date Telnet Manager is first launched. A reminder screen displays the time remaining for the Demo each time the TM1Config utility is launched.



The Demo is fully functional during this period. At the end of the trial period, Telnet Manager disables all client connections and does not allow any new connections.



Contact [Technical Assistance](#) (page 1) for information on obtaining a license key.

At any time after installation, a license key may be entered. Once the license key is entered:

- The Demo expiration message is no longer displayed at TM1Config startup.
- New client connections can be established.
- The DEMO notation in the Title Bar is removed and the License Registration branch is removed from the TM1Config utility.

## Launching Telnet Manager

### TM1Config Configuration Utility

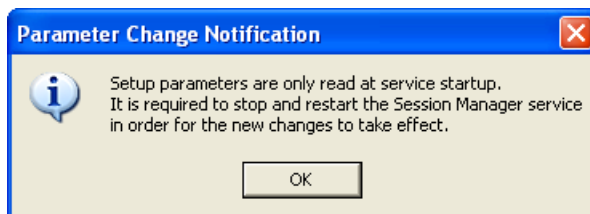
To launch the configuration utility, click on the TM1Config icon on the desktop or select **Start > All Programs > LXE > TM1-Config**.

*Note: This only launches the TM1Config utility. It does not start the Telnet Manager service.*

The configuration screens displayed depend on the Terminal Emulation selected during the installation process. Refer to the appropriate following sections for the installed Terminal Emulation:

- ANSI parameters are explained in [ANSI Configuration Utility](#) (page 39)
- IBM 3270 parameters are explained in [IBM 3270 Configuration Utility](#) (page 69)
- IBM 5250 parameters are explained in [IBM 5250 Configuration Utility](#) (page 89)

When parameter changes are made, you may see the following notification.



If this notification is displayed, follow the instructions in [TM1 Service](#) (page 29) to restart the service.

*Note: Restarting the service terminates any existing client connections.*

### TM1 Service

Telnet Manager's session management runs as a Windows service, identified as LXE TM1. The service is installed and configured to run automatically when Telnet Manager is installed. However, the TM1 service is not automatically started after installation.

Before starting the service, use the TM1Config utility to set the global parameters as desired. Once the changes are made using TM1Config, the service must be started (after initial install) or stopped and restarted (if TM1Config changes are made later). Use any of the methods detailed below to start/restart the service.



After installation, the TM1 Service cannot be started before launching the TM1Config utility.

## Starting/Restarting TM1 Service

The TM1 service will quit immediately if it is started prior to TM1Config being launched for the very first time. This action is taken in order to help ensure that the service is properly configured before running.

*Note: Stopping or restarting the service terminates any existing client connections.*

### Reboot

By default, the TM1 service Startup Type is set to Automatic. Even though the service is not started after Telnet Manager installation, the service is automatically started any time the Telnet Manager PC is rebooted.

### Use Restart Service Button

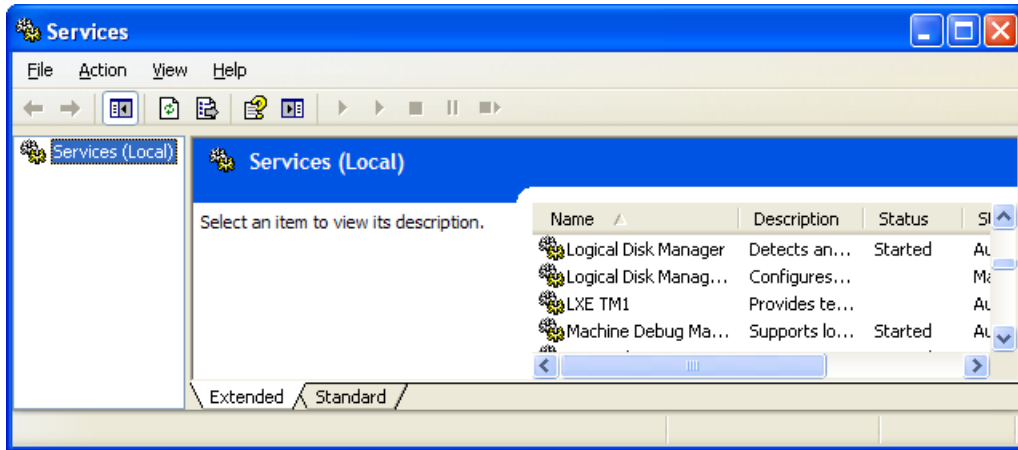
Clicking the **Restart Service** button on the Global Configuration screen restarts the TM1 service if it was previously running. If the service was not already running, clicking the **Restart Service** button starts the service. Restarting the service terminates any existing client connections.



---

## Use Windows Control Panel

The status of the TM1 service can be viewed and changed in the Windows Control Panel. To access the Services panel, select **Start > Control Panel > Administrative Tools > Services**. Locate and click the **LXE TM1** entry in the listed services. The Status column shows the current status of the service. If the service is started, links are provided to Stop or Restart the service. If the service is not running, a link is provided to Start the service.



*Note: Stopping or restarting the service terminates any existing client connections.*

Alternatively, the properties screen can be displayed for the service by double-clicking or right-clicking and selecting Properties. The service can be stopped or started from the Properties screen.

For more information on services, refer to Microsoft's Help feature or online documentation.

## Use TM1Console

TM1Console may be used to stop/start the service.

To use TM1Console, select **Start > Programs > LXE > TM1Console**.

If the TM1 service is not running, TM1Console displays a prompt to start the service.

If the TM1 service is running, use the stopService command to stop the service. Exit and restart TM1Console and follow the prompts to start the service.

Refer to [TM1Console](#) (page 31) for more details on TM1Console.

## Stopping TM1 Service

If it is necessary to stop the TM1 service, use one of the following methods:

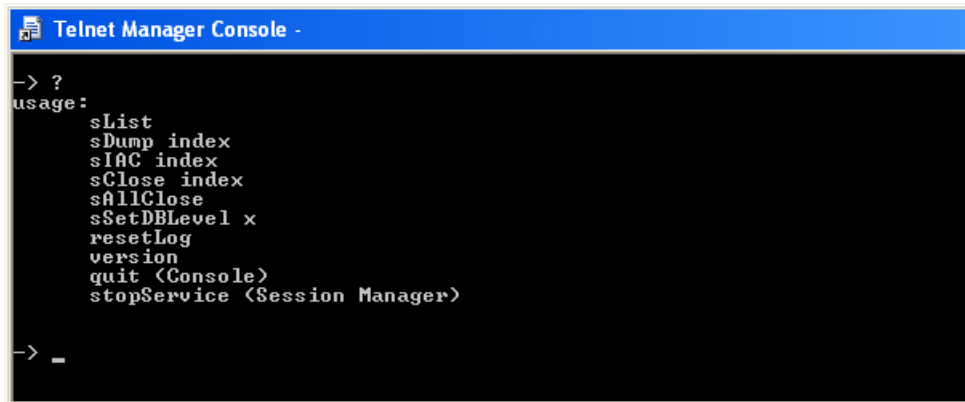
- [Use Windows Control Panel](#) (page 31) to locate and stop the TM1 service.
- Use the TM1 Console and the [stopService](#) (page 35) command to stop the TM1 service.

*Note: Stopping the service terminates any existing client connections.*

## TM1Console

TM1Console provides a command line window to the TM1 session manager service.

To use TM1Console, select **Start > Programs > Honeywell > Telnet Manager > TM1Console**.



Several functions are available in the TM1Console interface. When started, TM1Console checks to see if the windows service is running. If it is not running the following message is displayed:

The TM1 Service is not running. This console cannot run until it is started.

Do you wish to start it? [Y/N]

If "Y" is entered, the service starts. Otherwise, the service is not started and the command interface is closed after hitting the return key. No commands can be entered until the service is started.

## Commands

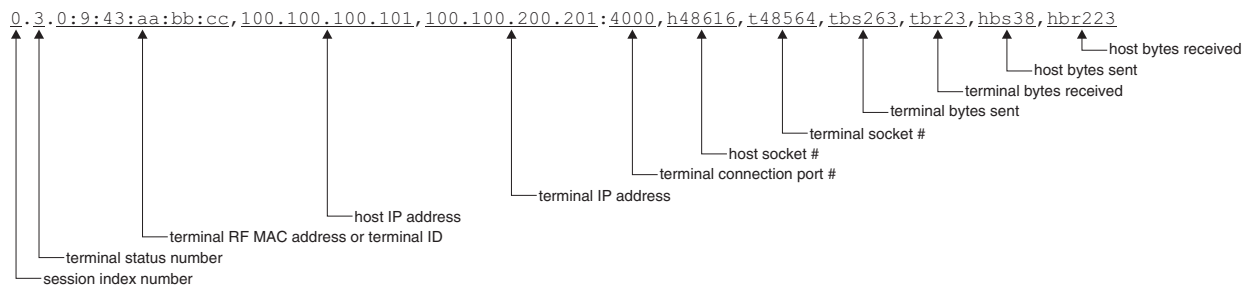
All commands are case sensitive. If an invalid command is entered, a list of valid commands is displayed.

### ?

The help command. Returns a list of the valid TM1Console commands. The list of commands is also displayed if an invalid command is entered.

### sList

Provides a list of all connected sessions and the associated status information for the session. Output is in the following format:

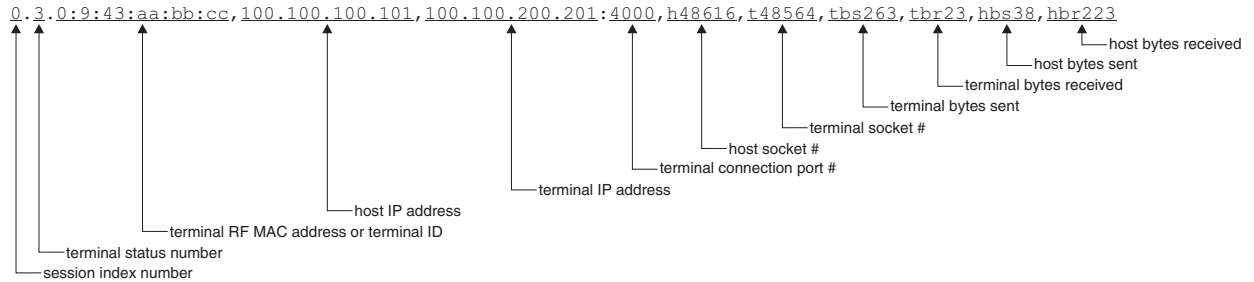


*Note: The index variable specified in the first position is used to specify the desired terminal for the sDump, sIAC and sClose commands.*

### sDump index

Provides detailed information on the terminal specified by the index parameter.

The first line of output is as follows:



Next, the telnet IAC command exchange between the terminal and the host is displayed. Lines that begin with terminalTelnetIACBuffers are the IAC commands received from the terminal. Lines that begin with hostTelnetIACBuffers are the IAC commands received from the host.

```
terminalTelnetIACBuffers[0] buflength = 3
[ 0xff 0xfb 0x18 ]
terminalTelnetIACBuffers[1] buflength = 11
[ 0xff 0xfa 0x18 0x0 VT220 0xff 0xf0 ]
terminalTelnetIACBuffers[2] buflength = 3
[ 0xff 0xfd 0x1 ]
terminalTelnetIACBuffers[3] buflength = 3
[ 0xff 0xfd 0x3 ]
terminalTelnetIACBuffers[4] buflength = 3
[ 0xff 0xfc 0x1 ]
hostTelnetIACBuffers[0] buflength = 3
[ 0xff 0xfd 0x18 ]
hostTelnetIACBuffers[1] buflength = 6
[ 0xff 0xfa 0x18 0x1 0xff 0xf0 ]
hostTelnetIACBuffers[2] buflength = 3
[ 0xff 0xfb 0x1 ]
hostTelnetIACBuffers[3] buflength = 3
[ 0xff 0xfb 0x3 ]
hostTelnetIACBuffers[4] buflength = 3
[ 0xff 0xfd 0x1 ]
hostTelnetIACBuffers[5] buflength = 3
[ 0xff 0xfe 0x1 ]
```

Next the buffers are listed with their status. If a terminal or a host Rx is pending for a buffer, the status is 1. Otherwise, the status is 0.

```
terminalOutDataBufIndex [0] 0
terminalOutDataBufIndex [1] 0
...
terminalOutDataBufIndex [24] 0
hostOutDataBufIndex [0] 0
hostOutDataBufIndex [1] 0
hostOutDataBufIndex [2] 0
hostOutDataBufIndex [3] 0
hostOutDataBufIndex [4] 0
terminalInDataBufIndex [0] 1
terminalInDataBufIndex [1] 0
terminalInDataBufIndex [2] 0
terminalInDataBufIndex [3] 0
terminalInDataBufIndex [4] 0
hostInDataBufIndex [0] 1
hostInDataBufIndex [1] 0
hostInDataBufIndex [2] 0
hostInDataBufIndex [3] 0
hostInDataBufIndex [4] 0
```

Finally, the contents of each buffer are displayed:

```
terminalOutDataBuf[0] buflength = 100
[ 0xff 0xfe 0x1 001:/usr4/users/tm0001> 0x20 9:51 0x20 from 0x20 172.16.91.2 0xd 0xa
SunOS 0x20 Release 0x20 4.1.3_U1
0x20 (CAE001) 0x20 #4: 0x20 Thu 0x20 Dec 0x20 27 0x20 11:]
terminalOutDataBuf[1] buflength = 100
[ 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
```

```

0x0 0x0 0x0 0x0 0x0 0x0 0x0
 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
0x0 0x0 0x0 0x0 0x0 0x0 0x0
 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
0x0 0x0 0x0 0x0 0x0 0x0 0x0
 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
0x0 0x0 0x0 0x0 0x0 0x0 0x0
 0x0 0x0 0x0 0x0 ]

```

...

```

hostInDataBuf[4] buflength = 100
[ 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
0x0 0x0 0x0 0x0 0x0 0x0 0x0
 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
 0x0 0x0 0x0 0x0 ]

```

### ***sIAC index***

Displays the telnet IAC command exchange between the terminal (identified by the specified index parameter) and the host. Lines that begin with terminalTelnetIACBuffers are the IAC commands received from the terminal. Lines that begin with hostTelnetIACBuffers are the IAC commands received from the host.

Sample output:

```

terminalTelnetIACBuffers[0] buflength = 3
[ 0xff 0xfb 0x18 ]
terminalTelnetIACBuffers[1] buflength = 11
[ 0xff 0xfa 0x18 0x0 VT220 0xff 0xf0 ]
terminalTelnetIACBuffers[2] buflength = 3
[ 0xff 0xfd 0x1 ]
terminalTelnetIACBuffers[3] buflength = 3
[ 0xff 0xfd 0x3 ]
terminalTelnetIACBuffers[4] buflength = 3
[ 0xff 0xfc 0x1 ]
hostTelnetIACBuffers[0] buflength = 3
[ 0xff 0xfd 0x18 ]
hostTelnetIACBuffers[1] buflength = 6
[ 0xff 0xfa 0x18 0x1 0xff 0xf0 ]
hostTelnetIACBuffers[2] buflength = 3
[ 0xff 0xfb 0x1 ]
hostTelnetIACBuffers[3] buflength = 3
[ 0xff 0xfb 0x3 ]
hostTelnetIACBuffers[4] buflength = 3
[ 0xff 0xfd 0x1 ]
hostTelnetIACBuffers[5] buflength = 3
[ 0xff 0xfe 0x1 ]

```

### ***sClose index***

Closes the socket connection between the terminal specified by the index parameter and the host.

### ***sAllClose***

Closes the socket connections between the terminal and host for all sessions.

### ***sSetDBLevel x***

Sets the level of debug information written to the debug log:

- x=6: debug messages off, error messages only (default).
- x=5: Least level of detail in debug log file.
- x=4: Intermediate level of detail in debug log file.
- x=3: Highest level of detail in debug log file.

The selected debug level is in effect only as long as the TM1Console remains open. When the TM1Console is closed, the debug log level returns to Off (no debug logging).

---

If the TM1 service is restarted, debugging returns to the default (Off) state however, there is no automatic indication that this change has been made.

***resetLog***

Closes the current debug log file and creates a new one.

***version***

Displays the revision level of the TM1 software plus the emulation selected during installation.

***quit***

Exits TM1Console. The TM1 service continues running.

***stopService***

Stops the TM1 service. Because the service is no longer running, no additional commands may be entered. The TM1-Console window is closed when return is pressed. Stopping the service terminates any existing client connections.

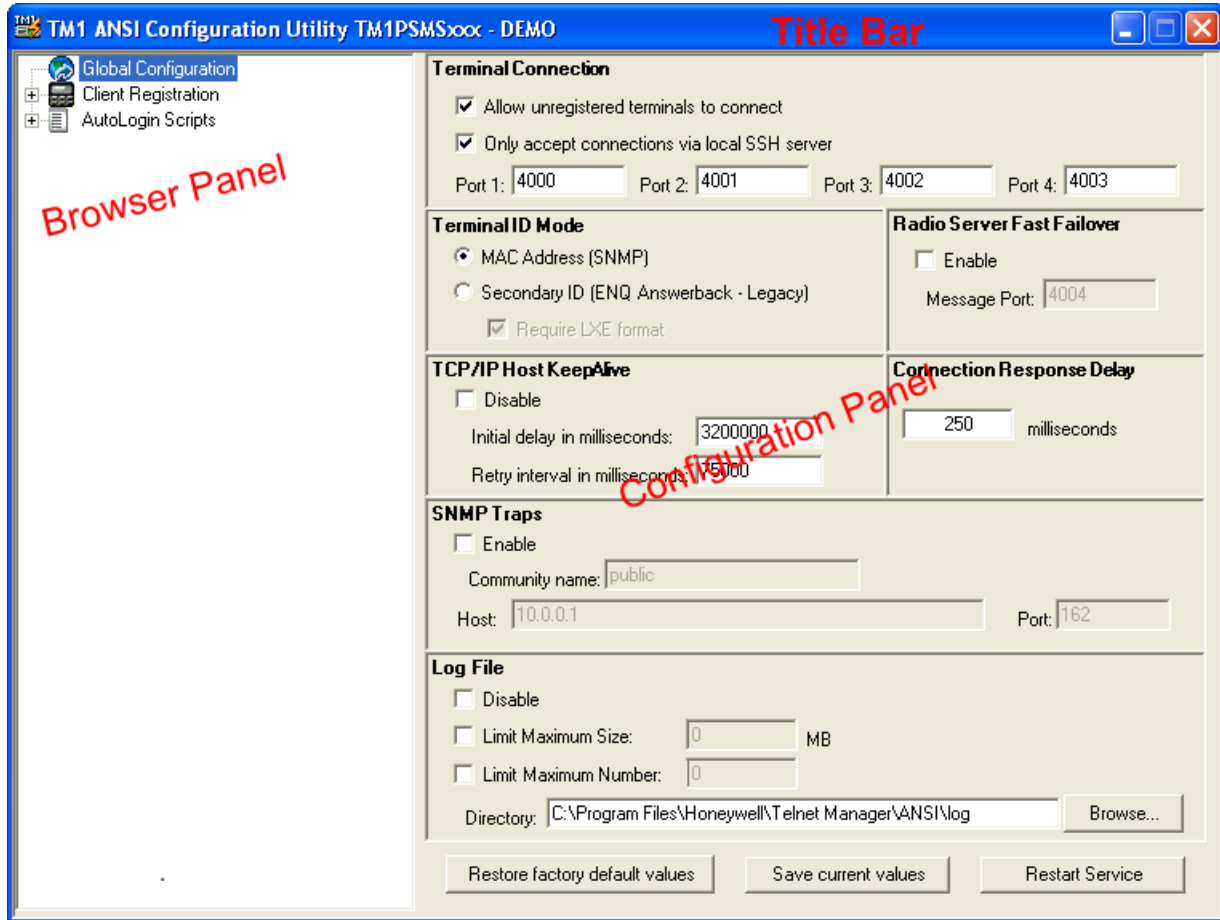
## ***Configuration Utility Interface***

TM1Config is the configuration utility used to set the session management parameters for Telnet Manager. The interface displayed is automatically selected based on the installed emulation.

### ***Components***

All versions of the configuration interface are modeled to a large extent upon the Windows Explorer paradigm. They all share three common components:

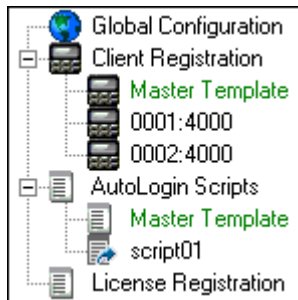
<b>Title Bar</b>	This component identifies the application. It also indicates the terminal emulation selected during installation and the software revision level of Telnet Manager. If Telnet Manager is running in Demo mode, the Title Bar also includes a DEMO notation.
<b>Browser Panel</b>	This component is located on the left side of the configuration interface display. It contains a tree-type representation of the components that can be managed. Contents of the Browser Panel vary according to the terminal emulation selected during installation.
<b>Configuration Panel</b>	This component occupies the right side of the configuration interface. It contains all the configurable items for the component selected in the Browser Panel. Screen contents vary depending on the terminal emulation selected during installation.



For all versions of the configuration interface, the coloring of the visual elements is based on the Windows desktop color scheme in effect. The only exceptions to this rule are the various icons used by the application.

### Browser Panel

The browser panel on the left side of the display indicates a tree structure containing all of the components that are associated with configurable parameters. The tree structure is collapsible and expandable by selecting the controls to the left of each component description.



*Note: The License Registration branch is displayed only when Telnet Manager is in Demo mode. Once a license key is entered, the License Registration branch is not displayed again.*















## Browser Panel Color Schemes

*Note: The color scheme of the browser panel is user configurable by modifying the Windows palette. The one exception to using standard Windows palette colors is for the unselected Master Template leaves.*

Background	Window Palette / Control
Unselected branch label	Window Palette / Control Text
Unselected leaf – except Master Template	Window Palette / Control Text
Unselected Master Template leaf	Green text on white background
Selected branch label	Window Palette / Selected Item
Selected leaf label	Window Palette / Selected Item
Mouse rollover branch label	Window Palette / Hot Track
Mouse rollover leaf label	Window Palette / Hot Track

## Icons

Branch and leaf icons are used to indicate the item status. Icons indicate if the item is selected or unselected. For the case of leaf items, the icon also indicates if the configuration of the leaf differs from the configuration of the Master Template for that branch.

	Global configuration branch – unselected
	Global configuration branch – selected
	Client registration branch – unselected
	Client registration branch – selected
	Registered client leaf – Master Template or same configuration as Master Template – unselected
	Registered client leaf – Master Template or same configuration as Master Template – selected
	Registered client leaf – different configuration from Master Template – unselected
	Registered client leaf – different configuration from Master Template – selected
	Autologin scripts branch – unselected
	Autologin scripts branch – selected
	Autologin scripts leaf – Master Template or same configuration as Master Template – unselected
	Autologin scripts leaf – Master Template or same configuration as Master Template – selected
	Autologin scripts leaf – different configuration from Master Template – unselected
	Autologin scripts leaf – different configuration from Master Template – selected

*Note: The icons may not appear exactly as shown in this guide.*

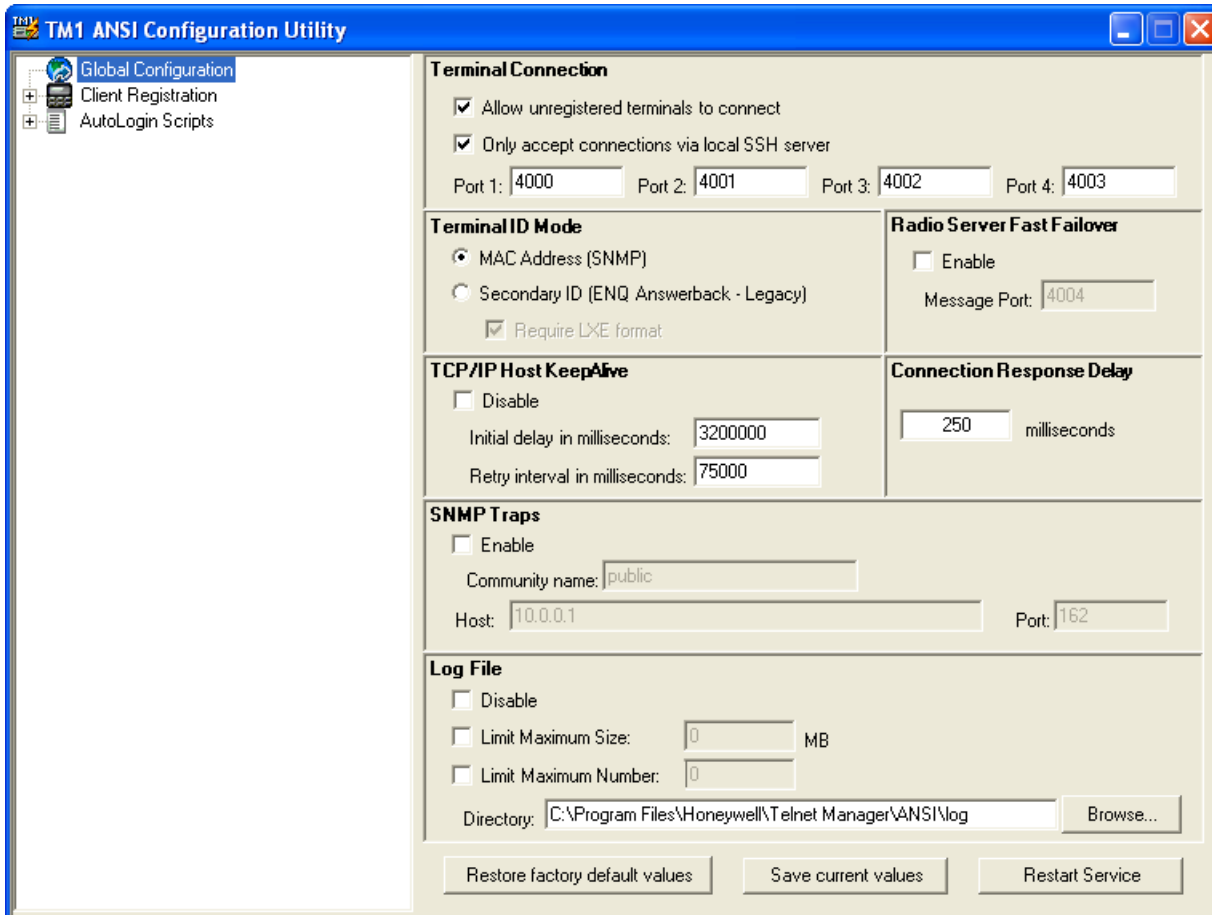




## ANSI Configuration Utility

### Introduction

The ANSI TM1Config configuration interface is launched by selecting **Start > Honeywell > Telnet Manager > TM1Config** or double-clicking the TM1Config icon on the desktop. This is the display that is shown first.



The Global Configuration branch of the browser tree is highlighted, and all the configurable global parameters (when selected) are displayed in the configuration panel.

## ANSI Telnet Manager Components

### Global Configuration

This branch contains no leaves. Global parameters are parameters that are independent of the individual client computers. These parameters affect the operation of Telnet Manager, the connection with the host computer or generally apply to all client devices.

### Client Registration

This branch contains the following leaves:

#### Client Registration Master Template Parameters

This leaf defines a template of client registration parameters that are applied by default to new client devices added to the Telnet Manager.

---

## **Client Registration Registered Client Parameters**

There is one of these leaves for each client computer identified to the ANSI Telnet Manager. These leaves are labeled using the identification string associated with the particular client computer. For ANSI session management, the identification string may be either a terminal ID string, or the radio MAC address.

### **AutoLogin Script**

This branch contains the following leaves:

#### **Master Autologin Parameters**

This leaf defines a template of autologin script parameters that are applied by default to new autologin scripts when they are first created.

#### **Individual Autologin Parameters**

There is one of these leaves for each autologin script defined to the ANSI Telnet Manager. These leaves are labeled using the name given to the autologin script when it was defined.

### **Registration License**

When Telnet Manager is running in Demo mode, the License Registration branch is displayed. If a valid key has previously been entered, this branch is no longer displayed.

This branch contains no leaves. The registration license key is entered on this screen to switch Telnet Manager from demo to licensed mode.

## **ANSI Global Configuration Parameters**

### **Factory Defaults**

Terminal Connection	Allow Unregistered Devices to Connect enabled Only accept connections via local SSH server (applicable only if WinSSHD is installed) Port 1 = 4000, Port 2 = 4001, Port 3 = 4002, Port 4 = 4003
Terminal ID Mode	MAC Address (SNMP)
Radio Server Fast Failover	Disabled. When enabled: Message Port = 4004
TCP/IP Host KeepAlive	Enabled. Initial delay: 7200000 milliseconds (2 hours) Retry interval: 75000 milliseconds (1.25 minutes)
Connection Response Delay	250 milliseconds
SNMP Traps	Disabled. When enabled: Community Name: 'public' Host: 10.0.0.1 Port: 162
Log File	Log file enabled, no limits on file size or number of log files. Location: <install directory>\ANSI\log i.e.: C:\Program Files\Honeywell\Telnet Manager\ANSI\log, or C:\Program Files (x86)\Honeywell\Telnet Manager\ANSI\log

### **Buttons**

#### **Restore Values to Factory Default**

Clicking this button causes all user modifiable fields to be restored to the factory default values.

---

## **Save current values**

Clicking this button causes all user modifiable fields displayed in this panel to be saved for use by the ANSI Telnet Manager.

These are the values that are displayed the next time the Global Configuration item in the browser tree is selected.

## **Restart Service**

Clicking this button stops and restarts the TM1 service. If the service is not already running, this button starts the service. Restarting the service terminates any existing client connections.

*Note: Restarting the service terminates any existing client connections.*

When global configuration data is changed, use the Restart Service button to restart the TM1 service using the changed parameters.

## **Parameters**

### **Terminal Connection**

#### **Allow Unregistered Terminals to Connect**

Typically, this option is used when setting up a system, for example when finding all client devices while configuring Telnet Manager. Once configured, and all client devices are registered with Telnet Manager, change this setting to not allow unregistered devices.

The checkbox controls the ability of client devices not previously registered with Telnet Manager to connect to Telnet Manager.

When selected, unregistered devices are allowed to connect to the host through the ANSI Telnet Manager. Selecting this checkbox also causes the configuration interface to refresh the browser panel display every ten seconds. This is done to constantly present a relatively current list of all connected client devices.

When not selected, connection attempts by unregistered devices are blocked. In this case, there is no need to refresh the browser panel.

Default is selected – unregistered devices are allowed to connect.

#### **Only Accept Connections via Local SSH Server**

*Note: This setting is applicable only if WinSSHD is installed.*

When selected, only incoming connections through the SSH server are allowed. When this option is selected and the Use SSH Tunnel option is selected on the Master Template, all Telnet Manager connections use SSH from end to end.

When not selected, standard telnet connections are accepted for incoming transmissions. Even if the Use SSH Tunnel option is selected, only the outgoing transmissions use SSH.

Default is selected – only accept connections via SSH server.

#### **Port 1 – 4**

These four text fields allow the user to specify the four TCP/IP ports the ANSI Telnet Manager listens to for client connection attempts.

Field edits are disabled if the port assigned to the field is in use by any of the defined client profiles.

Fields are validated for a legal port number (an integer in the range 1024 – 65535).

Default values are Port 1 = 4000, Port 2 = 4001, Port 3 = 4002, Port 4 = 4003.

*Note: On Windows XP SP2/SP3 or Windows Server 2003, the installation process configures the Windows firewall for Telnet Manager. If you are using a third-party firewall, you must manually open these ports or provide an exception for the Telnet Manager service.*

### **Terminal ID Mode**

#### **MAC Address (SNMP)**

If this option is selected, ANSI Telnet Manager uses the MAC address to identify the mobile device.

---

## Secondary ID (ENQ Answerback – Legacy)



This option must be enabled to use Radio Server Fast Failover.

If this option is selected, ANSI Telnet Manager uses legacy device identification mode (terminal ID strings from ENQ command response).

The Secondary ID mode *must* be selected when Telnet Manager is used to manage the MX8 with Windows Mobile.

### Require LXE Format

When the Secondary ID is selected, use this option to determine which devices can connect. This option is most useful in environments with poor wireless connectivity to the device.

If this option is enabled, the Secondary ID is required to be in the LXE format specified in RFTerm, for example:

```
LXE/q/24/RFTERMPXS1Tp/100.100.100.100
```

For more details on the LXE format, see **Use LXE Format** on the **Answerback** Tab in the VT Configuration section of the RFTerm Reference Guide.

When this option is checked, only devices with the LXE formatted ID are allowed to connect. When unchecked, any device can connect.

## Radio Server Fast Failover

Fast Failover is a Navis SPARCS feature that switches radio traffic to a backup radio server in the event the primary radio server fails. In general, Fast Failover allows the system to recover from a radio server failure automatically in two minutes or less. For complete information on the backbone necessary to support Fast Failover, refer to Navis' SPARCS Radio Server Fast Failover documentation.

*Note: SSH cannot be used with Fast Failover.*

### Enable

Check this box to enable the Fast Failover feature. The default value for this checkbox is deselected. Legacy mode [Secondary ID \(ENQ Answerback – Legacy\)](#) (page 42)) must be enabled to use Fast Failover. If Legacy Mode is not enabled, the Fast Failover checkbox cannot be checked.

### Message Port

This text field indicates the IP port number on the network manager station to receive control messages. The control message informs the TM1 to switch connections to the backup radio server. This field is validated for a legal port number (an integer in the range 1024 – 65535).

Default value for this field is 4004.

*Note: On Windows XP SP2/SP3 or Windows Server 2003, the installation process configures the Windows firewall for Telnet Manager. If you are using a third-party firewall, you must manually open these ports or provide an exception for the Telnet Manager service.*

## TCP/IP Host KeepAlive

The TCP/IP Host KeepAlive function prevents the TCP/IP socket connection between the application host and Telnet Manager from being torn down if the host is present. In a situation where there is no traffic between the host and Telnet Manager for a long time, Telnet Manager sends a KeepAlive message to the host computer. If the host responds, Telnet Manager knows the host is still present and keeps the socket open. If the host does not respond to repeated KeepAlive messages, Telnet Manager closes the socket to the host. This disables communications between the host and Telnet Manager until a new socket is negotiated. If Telnet Manager closes the host socket, it also closes the socket opened to the client computer as well. (With no host, there is no point in keeping the client connected.)

The Host KeepAlive function plays a role only if there has been no activity on the Telnet Manager / host link for a period of time. The Host KeepAlive timer is reset on every message received from the host computer. The Host KeepAlive function is useful to detect a failure on the host communications link during periods of inactivity. If the host connection is lost and Telnet Manager closes the socket, it also issues a Host KeepAlive SNMP Trap message.

---

Telnet session 'keep-alive' is controlled by three parameters:

Initial delay in milliseconds: This is the length of time of no activity from the host before sending the KeepAlive message.

Retry Interval in milliseconds: The length of time between KeepAlive message retries.

Disable Host KeepAlive: This parameter enables or disables the telnet session 'keep-alive' functionality.

### ***Disable***

This checkbox governs the host KeepAlive behavior of the ANSI Telnet Manager.

If the Host KeepAlive function is disabled, Telnet Manager does not send KeepAlive messages to the host computer, and does not close the socket to the host during periods of inactivity on the link.

When checked, the host KeepAlive is disabled. When checked, this control causes other data entry fields in this section to be disabled.

### ***Initial delay in milliseconds***

This text field indicates the duration of inactivity on the host link that Telnet Manager waits before sending a KeepAlive message to the host. The value is specified in milliseconds, and is validated for an integer number in the range 300,000 – 7,200,000.

Default value for this field is 7200000 milliseconds (2 hours).

### ***Retry interval (ms)***

This text field indicates the time to wait before sending another Terminal KeepAlive message if the client computer has not responded to the previous KeepAlive message(s). The client socket is closed, and a TE Disconnect SNMP trap is issued, if the client does not respond to 5 consecutive KeepAlive messages. The value of the "Retry interval in milliseconds" field is specified in milliseconds, and is validated for an integer number in the range 10,000 – 75,000.

Default value for this field is 75000 milliseconds (1.25 minutes).

### ***Connection Response Delay***

Provides a delay between when the computer connects to the Telnet Manager and when Telnet Manager issues the ENQ (inquiry) for the Answerback message from the computer.

This parameter is especially important when DOS computers are using the autoconnect feature to allow time for the emulator to respond. The value of the "Connection response delay" field is specified in milliseconds, and is validated for an integer number in the range 1 – 2,000.

Default value for this field is 250 milliseconds.

### ***SNMP Traps***

SNMP Traps are logged for the following actions:

Application host communications failure. An alarm event Trap is generated if Telnet Manager loses communications with any host for which a session is currently open.

Terminal communications failure. Telnet Manager generates an alarm event if a specific client device is disconnected due to a 'keep-alive' time out more than a specified number of times.

Telnet Manager Boot. When Telnet Manager goes through a Boot for whatever reason a "Boot Trap" is sent.

### ***Enable***

This checkbox controls the Telnet Manager SNMP Trap function.

When checked, Telnet Manager sends traps to the Trap Destination IP address (see below). When deselected, Telnet Manager does not send SNMP traps. When deselected, this control causes other data entry fields in this section to be disabled.

The default value for this checkbox is deselected.

---

### **Community Name**

This text field indicates the SNMP community name. This field is validated for a string with a maximum length of 32 characters.

Default value for this field is 'public'.

### **Host**

This text field indicates the IP address or Domain Name of the network manager that is to receive SNMP trap messages generated by the ANSI Telnet Manager. This field is NOT validated for correct IP address format (1.0.0.0 to 254.254.254.254).

Default value for this field is 10.0.0.1.

### **Port**

This text field indicates the IP port number on the network manager station to receive SNMP trap messages. This field is validated for a legal port number (an integer in the range 1 – 65535).

Default value for this field is 162.

## **Log File**

### **Disable**

When checked, no log file is kept.

The default is unchecked – a log file is maintained by Telnet Manager.

### **Limit Maximum Size**

This option determines the maximum file size (in MB) that Telnet Manager maintains for the log file. Once the maximum size is reached, Telnet Manager starts a new log file.

The default is unchecked – no limit on log file size.

To enable, check the box and specify a maximum file size in MB in the text box.

### **Limit Maximum Number**

This option determines the maximum number of log files that can accumulate before deleting the oldest log file. A new log file is created when either of the following occurs:

- The maximum file size is reached (see the parameter above)
- The Telnet Manager service is restarted.

The default is unchecked – no limit on the number of log files maintained.

To enable, check the box and specify the number of log files to keep.

### **Directory**

This text parameter holds the name of the directory path for the ANSI Telnet Manager log file. This field is validated to ensure the directory already exists.

Default value for this field is <install directory>\ANSI\LOG (when installed in the default directory, C:\Program Files\Honeywell\Telnet Manager\ANSI\log or C:\Program Files (x86)\Honeywell\Telnet Manager\ANSI\log).

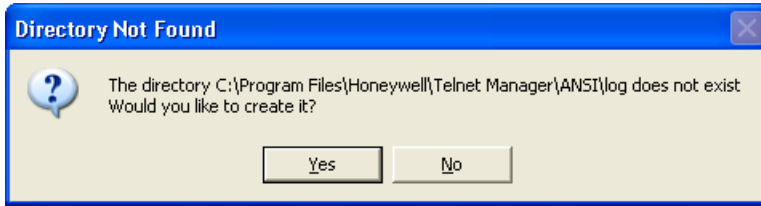
This field is validated to ensure the directory already exists.

The Browse button can be used to select a location for the log file.

## **Dialog / Error Boxes**

### **Directory Does Not Exist**

If the debug log file directory does not exist when the 'Save Current Values' button is clicked, a dialog box alerts the user and asks if the directory is to be created.



### **Select Yes**

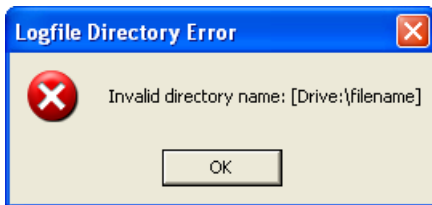
The directory specified in the Debug Log File Directory location is created and the dialog box is removed from the display.

### **Select No**

The directory specified in the Debug Log File Directory location control is not changed from the previously saved value. The dialog box is removed from the display.

### **Logfile Directory Error**

If the debug log file directory specified when the 'Save All Current Values' button is selected is not formatted as a valid directory string, a dialog box reminds the user of the format for a valid directory path.



### **Select OK**

The directory specified for the Debug Log File Directory location control is not changed from the previously saved value. The dialog box is removed from the display.

### **Select Close control**

Equivalent to the OK button.

### **Parameter Change Notification**

When the new Global Configuration parameters have been saved, a dialog box appears that states the new parameters do not take effect until the TM1Service is restarted.



### **Select OK**

The dialog box is removed from the display.

### **Select Close control**

Equivalent to the OK button.

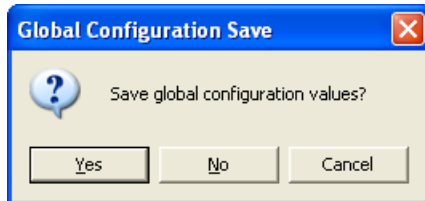
After dismissing the notification, to restart TM1Service, click the Restart Service button on the Global Configuration screen. For more information on TM1Service, including alternative methods of restarting the service, see [TM1 Service](#) (page 29).

*Note: Restarting the service terminates any existing client connections.*

---

## **Global Configuration Save**

If the Global Configuration item in the browser tree loses focus (some other item in the browser tree is selected or the ANSI TM1Config interface is closed), the panel is checked for unsaved changes. If any unsaved changes are detected, a dialog box is displayed to notify the user and request the desired action.



### **Select Yes**

All user modifiable fields displayed in this panel are saved for use by the ANSI Telnet Manager. These are the values that are displayed the next time the Global Configuration item in the browser tree is selected. The dialog box is removed from the display.

### **Select No**

The current session's user modified values in this panel are discarded and no changes are made. The previously saved values are displayed the next time the Global Configuration item in the browser tree is selected. The dialog box is removed from the display.

### **Select Cancel**

Focus is restored to the Global Configuration item in the browser panel and no changes are made.

None of the field values are altered and the dialog box is removed from the display.

### **Select Close control**

Equivalent to the Cancel button.

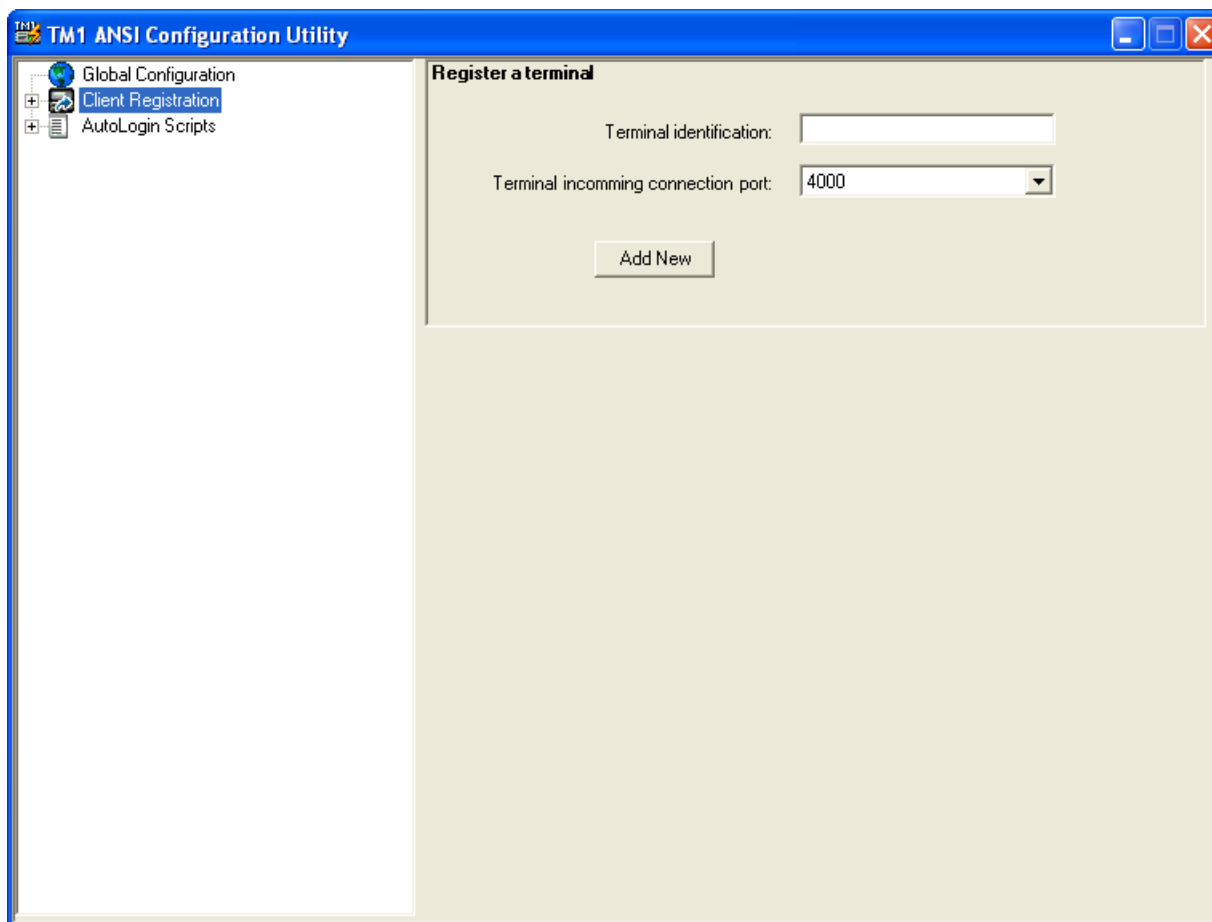
## **ANSI Client Registration**

Selecting the Client Registration item in the browser panel causes no action other than to highlight the Client Registration text and icon in the browser panel.

Selecting this choice causes the "Register a Terminal" interface to be displayed in the Register a terminal panel to appear.



## Registering New Client Devices



### Factory Defaults

Terminal Identification	Blank
Terminal incoming connection port	Value assigned to Port 1 in the Global Configuration panel.

### Buttons

#### Add New

Clicking this button causes the specified client identification string and port number to be added to the ANSI Telnet Manager database and the browser panel display is refreshed to include the newly defined client device.

Newly registered client devices are assigned configuration parameters from the Client Registration Master Template in effect at the time the device is registered. If the Terminal Identification field is blank, there is no action.

### Parameters

#### Terminal Identification

This text field stores the text string used to identify the new client device.

This field is validated to conform to a format consistent with the Terminal ID Mode selection on the Global Configuration screen.

- If MAC Address (SNMP) is selected, this field must be a text string formatted as a MAC address. MAC address format is six hexadecimal numbers in the range 0 through ff. Colon characters must separate the six numbers. They may be padded with leading zeros, but that is not required. MAC addresses are NOT case sensitive.

- If Secondary ID (ENQ Answerback- Legacy) is selected, this field must be a text string with a maximum length of 64 characters. Secondary IDs are NOT case sensitive. Also, since RFTerm can be configured to use its MAC address as its secondary ID, MAC addresses that were added to the list when the Terminal ID Mode was set to MAC Address are not filtered out when Terminal ID Mode switches to Secondary ID.

The default value of this field is blank.

### **Terminal Incoming Connection Port**

Select a port from the drop down list. Input is restricted to selecting from the pull-down list. If the value you need does not exist in the pull-down list, it must be added using the Global Configuration panel.

The default value of this field is the value assigned to Port 1 in the Global Configuration panel.

## **Client Registration / Master Template**

Selecting the 'Master Template' item in the browser panel list that is subordinate to Client Registration displays the Terminal Master Template interface in the configuration panel.

Using the mouse right-click function on the 'Master Template' item in the browser panel causes no action.

The screenshot shows the 'TM1 ANSI Configuration Utility' window. On the left is a tree view with 'Global Configuration', 'Client Registration', 'Master Template' (selected), and 'AutoLogin Scripts'. The main area is titled 'Master Template' and contains several sections:

- Host Connection:** Name: 10.0.0.1, Port: 23, Connection timeout (seconds): 10, Connection Management: Always maintain connection (default).
- Ssh:** Radio buttons for Off (selected), Shell, and Tunnel. Includes a 'Select Profile:' dropdown and an 'Edit/Create Profile' button.
- Activity Timeout:** An 'Enable' checkbox and a 'Timeout (minutes):' field set to 5.
- TCP/IP Terminal KeepAlive:** A 'Disable' checkbox, 'Initial delay (ms):' field set to 7200000, and 'Retry interval (ms):' field set to 75000.
- AutoLogin Script:** An 'Enable' checkbox, 'Select login script:' dropdown set to 'Master Template', and 'Timeout (seconds):' field set to 4.

At the bottom are two buttons: 'Restore factory default values' and 'Save current values'.

---

## Factory Defaults

Host Connection	Name: 10.0.0.1 Port: 23 Connection timeout in seconds: 10 seconds Connection Management: Always maintain connection
SSH	Off: Selected (SSH is disabled) Shell: Unselected Tunnel: Unselected Select Profile : N/A
Activity Timeout	Enable: Disabled Timeout (minutes): 5
TCP/IP Terminal KeepAlive	Disable: Enable Initial delay (ms): 7200000 milliseconds (2 hours) Retry interval (ms): 75000 milliseconds (1.25 minutes)
AutoLogin Script	Enable: Disabled Select autologin script: Master AutoLogin Template Timeout (seconds): 4

## Buttons

### **Edit/Create Profile**

This button is active only if SSH Tunnel or SSH Shell is selected. When active, this button accesses the [SSH Settings](#) (page 109) screen.

### **Restore Values to Factory Default**

Clicking this button causes all user modifiable fields to be restored to the factory default values.

### **Save current values**

Clicking this button causes all user modifiable fields displayed in this panel to be saved for use by the ANSI Telnet Manager.

These are the values that are displayed the next time the Client Registration / Master Template item in the browser tree is selected.

Values in the Master Template are automatically propagated to the registered terminals. All configuration items for all registered terminals that have not been changed from the Master Template values are immediately updated to reflect the new Master Template configuration. Configuration values for registered terminals that have been changed from the Master Template value are not affected.

## Parameters

### **Host Connection**

#### **Name**

Enter the IP address or Domain Name of the host computer to which this client device connects into this text field.

The default value of this field is 10.0.0.1.

#### **Port**

This text field indicates the IP port number on the application host to which this client device connects. This field is validated for a legal port number (an integer number in the range 1 – 65535).

Default value for this field is 23.

---

### **Connection Timeout (seconds)**

Enter the host connection timeout value for the client device in this text field. This field is validated for an integer in the range 5 – 65535.

Default value for this field is 10.

### **Connection Management**

Use this option to determine the type of Host Connection Management:

- Always close connection
- Always maintain connection (default)
- Close connection on explicit close.

### **SSH**

#### **Off**

Telnet is used without SSH.

#### **Shell**

A direct connection is made to the SSH server. When this box is checked, the Name field is set to the SSH Server Address and Port is set to the SSH Server Port. See [SSH Settings](#) (page 109). No Telnet connection is used.

#### **Tunnel**

A connection is established to an SSH server and Telnet traffic is tunneled (port forwarded) through the SSH connection.

*Note: This checkbox can only be accessed if the Include SSH option was selected during installation. Uninstall Telnet Manager and reinstall with the Include SSH option selected to enable this feature.*

### **Select Profile**

Select the name of a previously created SSH connection profile to use. If no profiles exist or to modify an existing profile, use the **Edit/Create Profile** button to access the [SSH Settings](#) (page 109) screen to create or modify a profile.

### **Activity Timeout**

The Activity Timeout allows the administrator to logoff a client computer that has been idle for a specified period of time. The client computer is logged off, and a Session Disconnect Activity timeout SNMP Trap is issued, regardless of whether or not the client computer is present on the network. Telnet Manager closes both the socket to the client computer and to the host computer. If this client computer subsequently reconnects to Telnet Manager, it is assigned to a new host session.

#### **Enable**

Selecting this checkbox enables the host-client activity timeout feature for this client device. If this checkbox is cleared, data entry in the Timeout in Minutes field is disabled.

The default state of this checkbox is not selected.

#### **Timeout (minutes)**

This text field is used to enter the host-client device activity timeout value for this client device. This field is validated for an integer in the range 5 – 65535.

If the Enable checkbox is not selected, data entry in this field is disabled.

Default value for this field is 5.

### **TCP/IP Terminal KeepAlive**

The TCP/IP Terminal KeepAlive function prevents the TCP/IP socket connection between the individual client computer and Telnet Manager from being torn down if the client computer is present. In a situation where there is no traffic between the client computer and Telnet Manager for a long time, Telnet Manager sends a KeepAlive message to the client. If the client responds, Telnet Manager knows the client is still present and keeps the socket

---

open. If the client computer does not respond to repeated KeepAlive messages, Telnet Manager closes the socket to the client computer. This disables communications between this particular client computer and Telnet Manager until a new socket is negotiated.

The Terminal KeepAlive function plays a role only if there has been no activity on the Telnet Manager / client computer link for a period of time. The Terminal KeepAlive timer is reset on every message received from the client computer. The Terminal KeepAlive function is useful to close unused client computer sockets. If the client computer connection is lost and Telnet Manager closes the socket, telnet Manager also issues a TE Disconnect SNMP Trap message.

Note that if Telnet Manager closes the client computer socket because the client does not respond to TCP/IP KeepAlive messages, it does not close the corresponding socket to the host computer. If the same client computer reconnects later, it is reconnected to the same host socket – that is, it is reconnected to the same session it had before.

### ***Disable***

This control governs the terminal KeepAlive behavior of the ANSI Telnet Manager.

When selected, terminal KeepAlive is disabled and causes the other data entry fields in this section to be disabled. If the Terminal KeepAlive function is disabled, Telnet Manager does not send KeepAlive messages to the client computer, and does not close the socket to the client during periods of inactivity on the link.

When cleared, terminal KeepAlive is enabled.

The default value for this checkbox is cleared.

### ***Initial delay (ms)***

This text field indicates the duration of inactivity on the client computer link that Telnet Manager waits before sending a KeepAlive message to the client. The value is specified in milliseconds, and is validated for an integer number in the range 300,000 – 7,200,000.

Default value for this field is the TCP/IP Terminal KeepAlive / Initial delay in milliseconds value from the Master Template or 7200000 milliseconds (2 hours).

### ***Retry interval (ms)***

This text field indicates the time to wait before sending another Terminal KeepAlive message if the client computer has not responded to the previous KeepAlive message(s). The client socket is closed, and a TE Disconnect SNMP trap is issued, if the client does not respond to five consecutive KeepAlive messages.

The value of this field is specified in milliseconds, and is validated for an integer number in the range 10,000 – 75,000.

Default value for this field is the TCP/IP Terminal KeepAlive / Retry interval in milliseconds value from the Master Template.

## ***AutoLogin Script***

This function essentially duplicates the autologin function found on the client devices. It enhances the device-based autologin capabilities by providing a centralized point of management. Each client device can have a unique autologin script maintained for it. Autologin scripts allow the client device to login to the host without user delays caused by typing in login names and passwords and/or application run commands. This capability is limited to the ANSI / ANSI Plus terminal emulation only.

### ***Enable AutoLogin***

Selecting this checkbox enables the autologin feature for this client device. If this checkbox is not selected, data entry in other fields in this section is disabled.

The default state of this checkbox is not selected.

### ***Select AutoLogin Script***

This pull-down list permits selecting an autologin script to use for this client device. List values include the Master AutoLogin Template and all user-defined autologin scripts.

The default value of this field is the Master AutoLogin Template.

---

Input is restricted to selecting from the pull-down list.

### ***Timeout (seconds)***

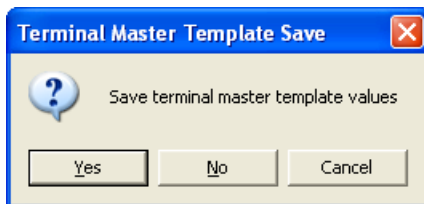
This text field allows the user to enter the login timeout value in seconds. This field is validated for an integer in the range 4 – 65535.

The default value for this field is 4 seconds.

## ***Dialog / Error Boxes***

### ***Terminal Master Template Save***

If the Client Registration Master Template item in the browser tree loses focus (some other item in the browser tree is selected or the ANSI TM1Config interface is closed), the panel is checked for unsaved changes. If any unsaved changes are detected, a dialog box is displayed to notify the user and request the desired action.



#### ***Select Yes***

All user modifiable fields displayed in this panel are saved for use by the ANSI Telnet Manager. These are the values that are displayed the next time the Client Registration Master Template item in the browser tree is selected. The dialog box is removed from the display.

#### ***Select No***

The current session's user modified values in this panel are discarded and no changes are made. The previously saved values are displayed the next time the Client Registration Master Template item in the browser tree is selected. The dialog box is removed from the display.

#### ***Select Cancel***

Focus is restored to the Client Registration Master Template item in the browser panel and no changes are made.

None of the field values are altered and the dialog box is removed from the display.

#### ***Select Close control***

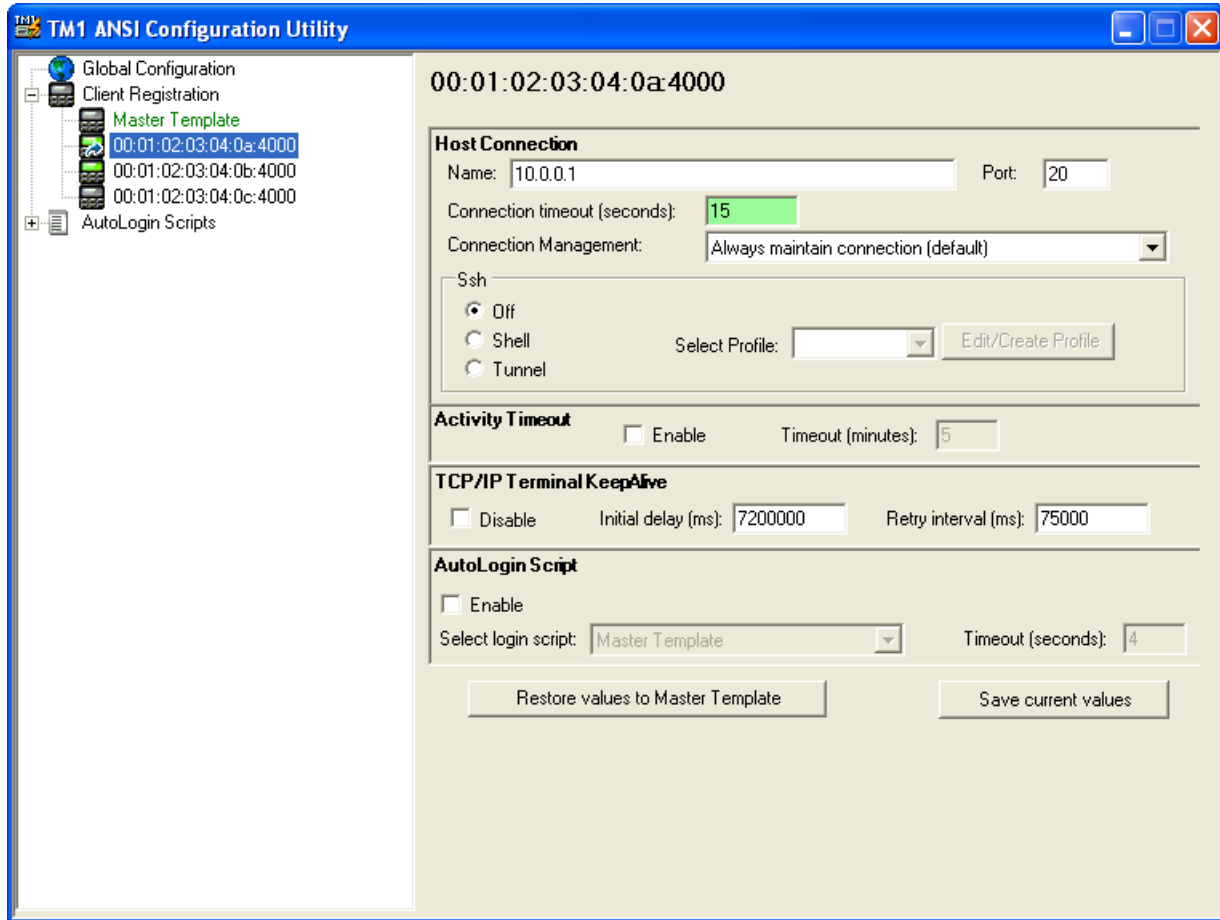
Equivalent to the Cancel button.

## ***Client Registration / Registered Clients***

Selecting any of the individual client ID items in the browser panel list subordinate to Client Registration displays the Registered Terminal interface in the configuration panel.

If any of the configurable parameters in this configuration panel display differ from the corresponding parameters in the Master Template configuration panel, those controls are highlighted. Likewise the Registered Client icon is also highlighted for any clients whose saved values differ from the Master Template values.

A right mouse click on the selected individual client ID item, displays a one-line menu item – to delete the highlight registered client. Refer to [Removing a Registered Client](#) (page 57) for instructions.



---

## Factory Defaults

Host Connection	Name: Host Connection IP address of the host computer from the Master Template. Port: Host Connection Port value from the Master Template. Connection timeout in seconds: Host Connection Timeout value From the Master Template. Connection Management: Value from the Master Template.
SSH	Off, Shell, Tunnel: Value from the Master Template Select Profile: Value from the Master Template
Activity Timeout	Enable: Activity Timeout Enable checkbox from the Master Template. Timeout (minutes): Activity Timeout / Timeout in Minutes value from the Master Template.
TCP/IP Terminal KeepAlive	Disable: Disable checkbox status from the Master Template. Initial delay (ms): TCP/IP Terminal KeepAlive / Initial delay in milliseconds value from the Master Template. Retry interval (ms): TCP/IP Terminal KeepAlive / Retry interval in milliseconds value from the Master Template.
AutoLogin Script	Enable: State of the AutoLogin Script Enable checkbox from the Master Template. Select autologin script: Select AutoLogin Script value from the Master Template. Timeout (seconds): Timeout in Seconds value from the Master Template.

## Buttons

### **Edit/Create Profile**

This button is active only if SSH Tunnel or SSH Shell is selected. When active, this button accesses the [SSH Settings](#) (page 109) screen.

### **Restore Values to Master Template**

Clicking this button causes all user modifiable fields to be restored to the values defined by the current Client Configuration Master Template.

### **Save current values**

Clicking this button causes all user modifiable fields displayed in this panel to be saved for use by the ANSI Telnet Manager.

These are the values that are displayed the next time this Client ID is selected in the Client Registration branch of the browser tree.

## Parameters

In some cases, system administrators are concerned about having client devices logged in but inactive. In these cases, Telnet Manager provides the ability to log the client device off the host if there has been no user activity for a specified time period. The parameters used to manage RF client devices are Host Connection, Manage Terminal Sessions, and Activity Timeout.

### **Host Connection**

#### **Name**

Enter the IP address or Domain Name of the host computer to which this client device connects into this text field. This field is validated for correct IP address format (1.0.0.0 to 254.254.254.254).

The default value of this field is the Host Connection IP Address value from the Master Template.

#### **Port**

This text field indicates the IP port number on the application host to which this client connects. This field is validated for a legal port number (an integer number in the range 1 – 65535).



---

Default value for this field is the Host Connection Port value from the Master Template.

*Note: If Use SSH Tunnel (see below) is selected, the value in this field must be set to the listening port specified in the SSH profile.*

### **Connection Timeout (seconds)**

Enter the host-client connection timeout value in this text field. This field is validated for an integer in the range 5 – 65535.

Default value for this field is the Host Connection Timeout in Seconds value from the Master Template.

### **Connection Management**

Use this option to determine the type of Connection Management:

- Always close connection
- Always maintain connection (default)
- Close connection on explicit close.

### **SSH**

Default value for SSH is the connection type from the Master Template.

#### **Off**

Telnet is used without SSH.

#### **Shell**

A direct connection is made to the SSH server. When this box is checked, the Name field is set to the SSH Server Address and Port is set to the SSH Server Port. See [SSH Settings](#) (page 109). No Telnet connection is used.

#### **Tunnel**

A connection is established to an SSH server and Telnet traffic is tunneled (port forwarded) through the SSH connection.

*Note: If this option is enabled on the Client Registration Master Template, the default SSH tunnel is created at TM1 startup. If a different SSH tunnel connection profile is used for a registered terminal, there may be a delay when first connecting as it can take up to 20 seconds to establish an SSH tunnel.*

### **Select Profile**

Select the name of a previously created SSH connection profile to use. If no profiles exist or to modify an existing profile, use the **Edit/Create Profile** button to access the [SSH Settings](#) (page 109) screen.

The default value is the profile (if any) from the Master Template.

### **Activity Timeout**

#### **Enable**

Selecting this checkbox enables the activity timeout feature for this client device. If this checkbox is cleared, data entry in the Timeout in Minutes field is disabled.

Default state for this checkbox is the state of the Activity Timeout Disable checkbox from the Master Template.

#### **Timeout (minutes)**

This text field is used to enter the activity timeout value for this client device. This field is validated for an integer in the range 5 – 65535.

Default value for this field is the Activity Timeout / Timeout in Minutes value from the Master Template.

### **TCP/IP Terminal KeepAlive**

The TCP/IP Terminal KeepAlive function prevents the TCP/IP socket connection between the individual client computer and Telnet Manager from being torn down if the client computer is present. In a situation where there is no traffic between the client computer and Telnet Manager for a long time, Telnet Manager sends a KeepAlive message to the client. If the client responds, Telnet Manager knows the client is still present and keeps the socket

---

open. If the client computer does not respond to repeated KeepAlive messages, Telnet Manager closes the socket to the client computer. This disables communications between this particular client computer and Telnet Manager until a new socket is negotiated.

The Terminal KeepAlive function plays a role only if there has been no activity on the Telnet Manager / client computer link for a period of time. The Terminal KeepAlive timer is reset on every message received from the client computer. The Terminal KeepAlive function is useful to close unused client computer sockets. If the client computer connection is lost and Telnet Manager closes the socket, Telnet Manager also issues a TE Disconnect SNMP Trap message.

Note that if Telnet Manager closes the client computer socket because the client does not respond to TCP/IP KeepAlive messages, it does not close the corresponding socket to the host computer. If the same client computer reconnects later, it is reconnected to the same host socket – that is, it is reconnected to the same session it had before.

### ***Disable***

This control governs the terminal KeepAlive behavior of the ANSI Telnet Manager.

When selected, terminal KeepAlive is disabled and causes the other data entry fields in this section to be disabled. If the Terminal KeepAlive function is disabled, Telnet Manager does not send KeepAlive messages to the client computer, and does not close the socket to the client during periods of inactivity on the link.

When cleared, terminal KeepAlive is enabled.

The default value for this field is the Disable checkbox status from the Master Template.

### ***Initial Delay***

This text field indicates the duration of inactivity on the client computer link that Telnet Manager waits before sending a KeepAlive message to the client. The value is specified in milliseconds, and is validated for an integer number in the range 300,000 – 7,200,000.

Default value for this field is the TCP/IP Terminal KeepAlive / Initial delay in milliseconds value from the Master Template or 7200000 milliseconds (2 hours).

### ***Retry interval (ms)***

This text field indicates the time to wait before sending another Terminal KeepAlive message if the client computer has not responded to the previous KeepAlive message(s). The client socket is closed, and a TE Disconnect SNMP trap is issued, if the client does not respond to five consecutive KeepAlive messages.

The value of this field is specified in milliseconds, and is validated for an integer number in the range 10,000 – 75,000.

Default value for this field is the TCP/IP Terminal KeepAlive / Retry interval in milliseconds value from the Master Template.

## ***AutoLogin Script***

This function essentially duplicates the autologin function found on the client devices. It enhances the device-based autologin capabilities by providing a centralized point of management. Each client device can have a unique autologin script maintained for it. Autologin scripts allow the client device to login to the host without user delays caused by typing in login names and passwords and/or application run commands. This capability is limited to the ANSI / ANSI Plus terminal emulation only.

### ***Enable AutoLogin***

Selecting this checkbox enables the autologin feature for this client device. If this checkbox is not selected, data entry in other fields in this section is disabled.

Default state for this checkbox is the state of the AutoLogin Script Enable checkbox from the Master Template.

### ***Select AutoLogin Script***

This pull-down list permits selecting an autologin script to use for this client device. List values include the Master AutoLogin Template and all user-defined autologin scripts.

The default value of this field is the Select AutoLogin Script value from the Master Template.

---

Input is restricted to selecting from the pull-down list.

### ***Timeout (seconds)***

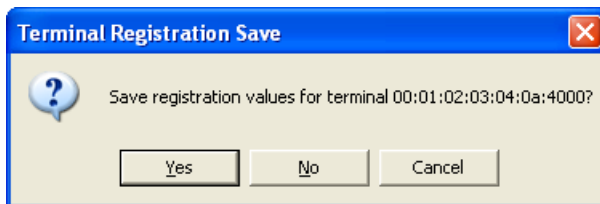
This text field allows the user to enter the login timeout value in seconds. This field is validated for an integer in the range 4 – 65535.

The default value for this field is the Timeout in Seconds value from the Master Template.

## ***Dialog / Error Boxes***

### ***Terminal Registration Save***

If the Client Registration individual client ID item in the browser tree loses focus (some other item in the browser tree is selected or the ANSI TM1Config interface is closed), the panel is checked for unsaved changes. If any unsaved changes are detected, a dialog box is displayed to notify the user and request the desired action.



#### ***Select Yes***

All user modifiable fields displayed in this panel are saved for use by the ANSI Telnet Manager. These are the values that are displayed the next time this individual client ID item in the browser tree is selected. The dialog box is removed from the display.

#### ***Select No***

The current session's user modified values in this panel are discarded and no changes are made. The previously saved values are displayed the next time this individual client ID is selected. The dialog box is removed from the display.

#### ***Select Cancel***

Focus is restored to the Client Registration Master Template in the browser panel and no changes are made. None of the field values are altered and the dialog box is removed from the display.

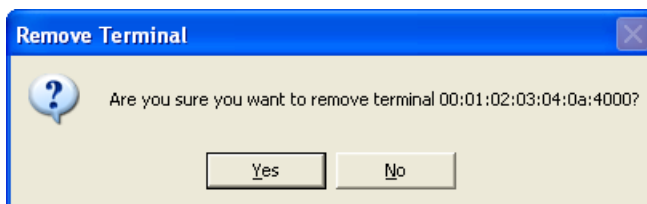
#### ***Select Close control***

Equivalent to the Cancel button.

### ***Removing a Registered Client***

Using the mouse right-click function in the browser panel when one of the individual client ID items has focus (is highlighted) causes an option menu to be displayed.

The option menu contains the single choice to remove the selected client. Selecting this choice causes the "Remove Terminal" dialog box to be displayed. The dialog box requests user confirmation to remove the selected terminal registration. The individual client ID text and icon retain their highlighted (selected) status until the removal is confirmed.



---

### **Select Yes**

Selecting this option causes the specified terminal registration to be removed and entries for this terminal are removed and are no longer available to the ANSI Telnet Manager. The browser panel is refreshed to show the browser tree without the removed terminal. Focus in the browser panel shifts to the terminal that previously followed the removed terminal.

If the removed terminal was the last terminal in the list, focus shifts to the preceding terminal in the list. If the removed terminal was the only terminal in the list, focus shifts to the Client Registration Master Template

The configuration panel is refreshed to reflect the item now selected in the browser panel and the Remove Terminal dialog box is removed from the display.

### **Select No**

The specified terminal registration is retained and the Remove Terminal dialog box is removed from the display.

## **ANSI AutoLogin Scripts**

ANSI AutoLogin scripts essentially duplicate the autologin function found on client devices. It enhances the device-based autologin capabilities by providing a centralized point of management. Each client device can have a unique autologin script maintained for it. Autologin scripts allow the client device to login to the host without delays caused by manually typing login names, passwords and/or application run commands. This capability is limited to the ANSI / ANSI Plus terminal emulation only.

*Note: When using SSH Shell, the login is handled by the SSH profile. AutoLogin should not be used unless it is needed to log into an application launched from the shell on the SSH server.*

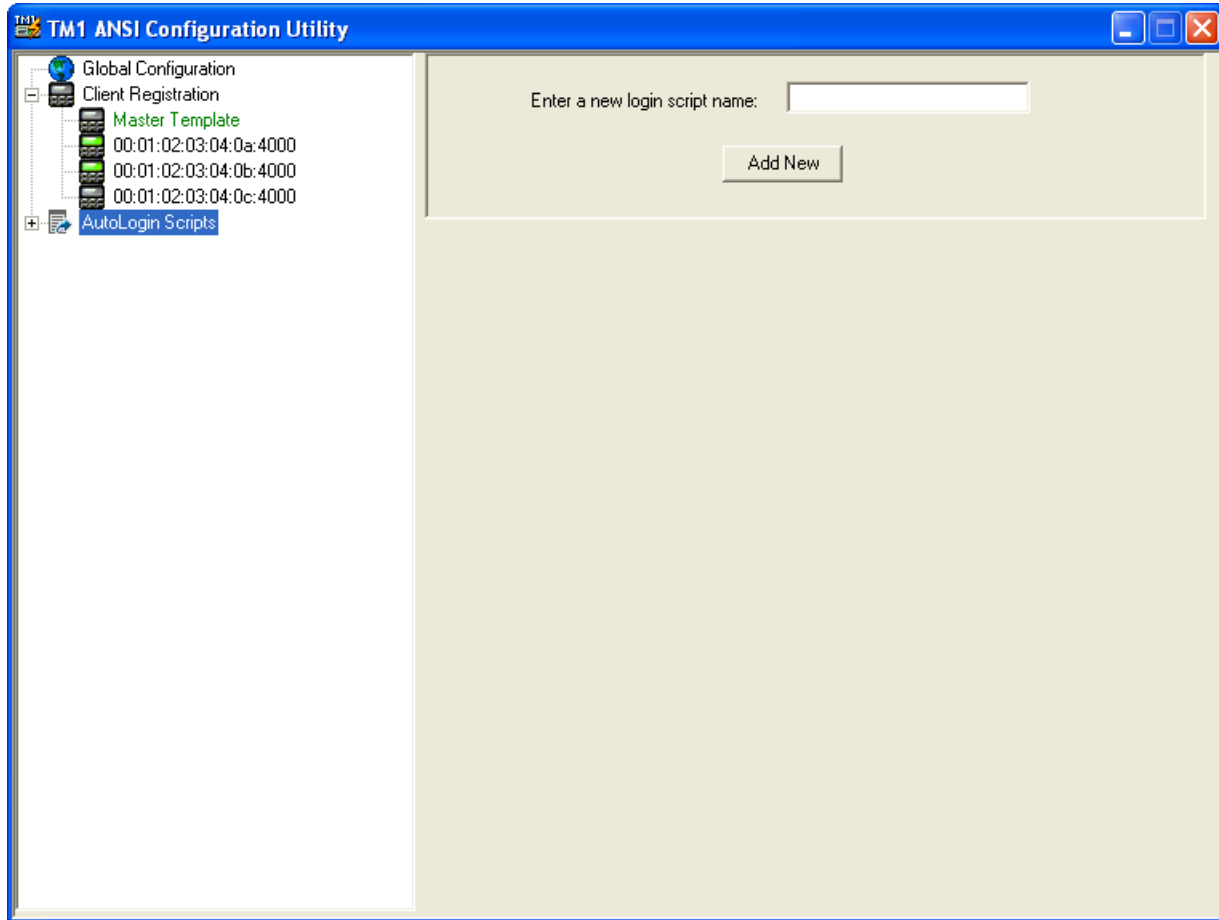
Host data is not displayed on the client device screen until the autologin process is completed successfully. Six parameters are available:

First prompt	Normally text sent from the host and displayed on the client device screen e.g. Login:. The host waits for a response from the client device user.
First response	Normally text typed by the client device user e.g. user login name. The text is sent to the host when the Enter key is pressed.
Second prompt	The second prompt is displayed after the host evaluates and validates the data sent from the client device user as their First response. The second prompt is normally text sent from the host and displayed on the client device screen e.g. Password:. The host waits for a response from the client device user.
Second response	Normally text typed by the client device user e.g. user assigned password. The text is sent to the host when the Enter key is pressed.
Third, fourth, fifth and sixth prompt	The third through sixth prompts are displayed after the host evaluates and validates the data sent from the client device user as their Second response. These prompts are normally text sent from the host and displayed on the client device screen e.g. Application to Run:. The host waits for a response from the client device user.
Third, fourth, fifth and sixth response	Normally text typed by the client device user e.g. an application run command or a string of text to look for in the incoming host data stream. The text is sent to the host when the Enter key is pressed. The host then evaluates and validates the Third through sixth response text strings and, if an application run command was sent, the application begins.

Selecting the AutoLogin Scripts item in the browser panel displays the “New Login Script” interface in the configuration panel.

### **Creating New AutoLogin Scripts**

Using the mouse right-click function while the AutoLogin Scripts item in the browser panel is highlighted displays an option menu. The option menu contains the single choice to add a new login script.



## **Buttons**

### **Add New**

Clicking this button causes the specified login script identification string to be added to the ANSI Telnet Manager database and the browser panel display is refreshed to include the newly defined login script.

Newly created login scripts are assigned configuration parameters from the AutoLogin Scripts Master Template in effect at the time the device is registered.

When the Enter a New Login Script Name field is blank, there is no action.

## **Parameters**

### **Enter a New Login Script Name**

This text field is used to enter the name of the new login script. This field is validated for a 32 character maximum string.

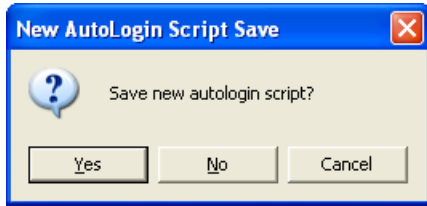
The default value of this field is blank.

## **Dialog Boxes / Errors**

### **New AutoLogin Script Save**

If the AutoLogin Scripts item in the browser tree loses focus (some other item in the browser tree is selected or the ANSI TM1Config interface is closed) while the Create New AutoLogin Script interface is displayed in the configuration panel, the configuration panel is checked for unsaved changes.

If any unsaved changes are detected, a dialog box is displayed to notify the user and request the desired action.



**Select Yes**

The new autologin script name specified in the Create New AutoLogin Script interface panel is saved for use by the ANSI Telnet Manager and the browser panel display is refreshed to include the newly defined login script. Newly created login scripts are assigned configuration parameters from the AutoLogin Scripts Master Template in effect at the time the device is registered. The dialog box is removed from the display.

**Select No**

The new autologin script name is discarded and no changes are made. The dialog box is removed from the display.

**Select Cancel**

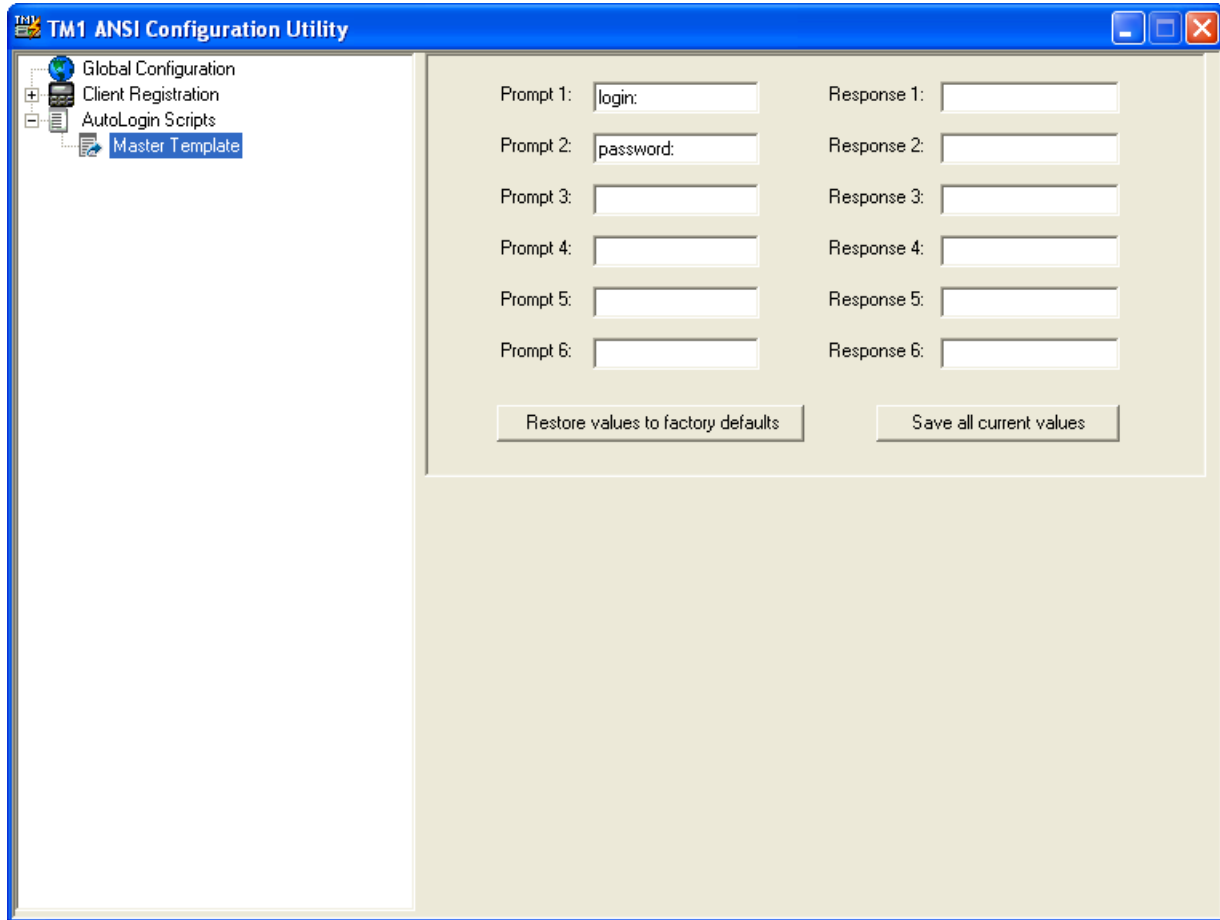
Focus is restored to the AutoLogin Scripts item in the browser panel and no changes are made. None of the field values are altered and the dialog box is removed from the display.

**Select Close control**

Equivalent to the Cancel button.

**AutoLogin Scripts / Master Template**

Selecting the 'Master Template' item in the browser panel list that is subordinate to Autologin Scripts displays the AutoLogin Scripts Master Template interface in the configuration panel. Using the mouse right-click function on the 'Master Template' item in the browser panel causes no action.



*Note: When autologin string is entered in RFTerm, the carriage return/life feed is added using hat encoding. It is not necessary to add the CR/LF in Telnet Manager as it is added automatically to the strings.*

---

## **Factory Defaults**

First Prompt	"login:"
First Response	Empty string
Second Prompt	"password:"
Second Response	Empty string
Third Prompt	Empty string
Third Response	Empty string
Fourth Prompt	Empty string
Fourth Response	Empty string
Fifth Prompt	Empty string
Fifth Response	Empty string
Six Prompt	Empty string
Six Response	Empty string

## **Buttons**

### ***Restore values to factory defaults***

Selecting this button resets all user modifiable fields on the AutoLogin Script Master Template to the default values.

### ***Save current values***

Clicking this button causes all user modifiable fields displayed in this panel to be saved for use by the ANSI Telnet Manager. These are the values that are displayed the next time the AutoLogin Scripts / Master Template item in the browser tree is selected.

## **Parameters**

### ***First prompt***

This text field allows the user to enter the first string of text to look for in the incoming host data stream. This field is a string with maximum length of 64 characters. The default value of this field is "login:".

### ***First Response***

This text field indicates the text string that should be sent back to the host when the "First prompt" string is encountered. This field is a string with maximum length of 64 characters. Default value for this field is an empty string.

### ***Second Prompt***

This text field allows the user to enter the second string of text to look for in the incoming host data stream. This field is a string with maximum length of 64 characters. The default value of this field is "password:".

### ***Second Response***

This text field indicates the text string that should be sent back to the host when the "Second Prompt" string is encountered. This field is a string with maximum length of 64 characters. Default value for this field is an empty string.

### ***Third Prompt***

This text field allows the user to enter a third string of text to look for in the incoming host data stream. This field is a string with maximum length of 64 characters. The default value of this field is an empty string.



---

### **Third Response**

This text field indicates the text string that should be sent back to the host when the “Third Prompt” string is encountered. This field is a string with maximum length of 64 characters. Default value for this field is an empty string.

### **Fourth Prompt**

This text field allows the user to enter a fourth string of text to look for in the incoming host data stream. This field is a string with maximum length of 64 characters. The default value of this field is an empty string.

### **Fourth Response**

This text field indicates the text string that should be sent back to the host when the “Fourth Prompt” string is encountered. This field is a string with maximum length of 64 characters. Default value for this field is an empty string.

### **Fifth Prompt**

This text field allows the user to enter a fifth string of text to look for in the incoming host data stream. This field is a string with maximum length of 64 characters. The default value of this field is an empty string.

### **Fifth Response**

This text field indicates the text string that should be sent back to the host when the “Fifth Prompt” string is encountered. This field is a string with maximum length of 64 characters. Default value for this field is an empty string.

### **Sixth Prompt**

This text field allows the user to enter a sixth string of text to look for in the incoming host data stream. This field is a string with maximum length of 64 characters. The default value of this field is an empty string.

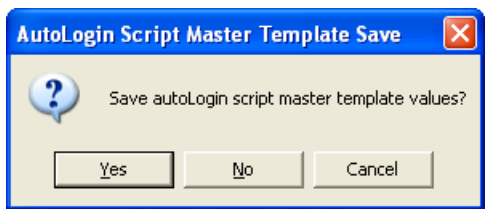
### **Sixth Response**

This text field indicates the text string that should be sent back to the host when the “Sixth Prompt” string is encountered. This field is a string with maximum length of 64 characters. Default value for this field is an empty string.

## **Dialog Boxes / Errors**

### **AutoLogin Script Master Template Save**

If the AutoLogin Scripts Master Template item in the browser tree loses focus (some other item in the browser tree is selected or the ANSI TM1Config interface is closed), the panel is checked for unsaved changes. If any unsaved changes are detected, a dialog box is displayed to notify the user and request the desired action.



#### **Select Yes**

All user modifiable fields displayed in the AutoLogin Scripts Master Template interface panel are saved for use by the ANSI Telnet Manager. These are the values that are displayed the next time the AutoLogin Scripts Master Template item in the browser tree is selected. The dialog box is removed from the display.

#### **Select No**

All user modified values in this panel are discarded and no changes are made. The most recently saved values are displayed the next time the AutoLogin Scripts Master Template is selected. The dialog box is removed from the display.

### **Select Cancel**

Focus is restored to the AutoLogin Scripts Master Template item in the browser panel and no changes are made.

None of the field values are altered and the dialog box is removed from the display.

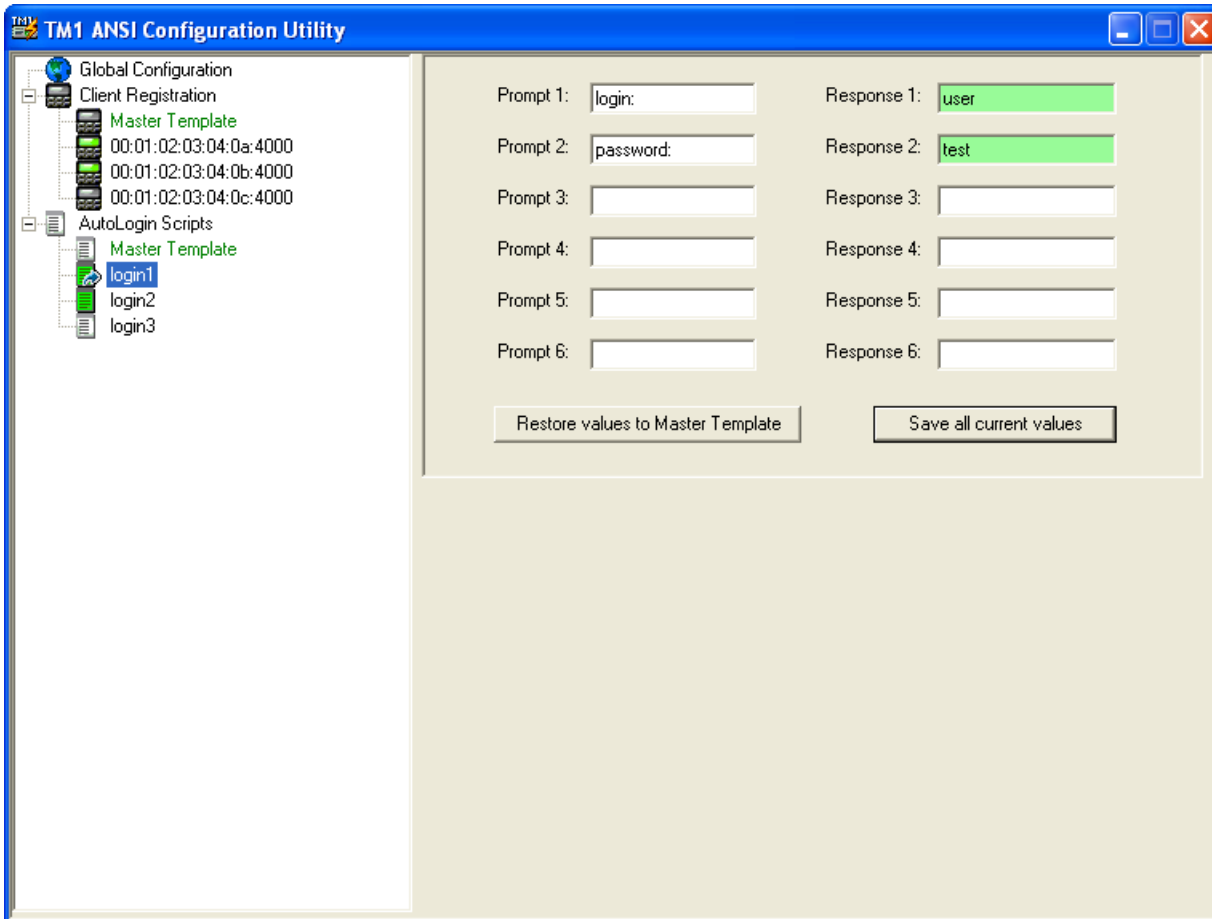
### **Select Close control**

Equivalent to the Cancel button.

## **AutoLogin Scripts / Named Scripts**

Selecting any of the individual autologin script name items in the browser panel list that is subordinate to AutoLogin Scripts displays the Named AutoLogin Scripts interface in the configuration panel.

If any of the configurable parameters in this configuration panel display differ from the corresponding parameters in the Master Template configuration panel, the parameters are highlighted. Likewise the Autologin Script icon is also highlighted for any scripts whose saved values differ from the Master Template values.



### **Buttons**

#### **Restore values to Master Template**

Clicking this button resets all user modifiable fields on the Named AutoLogin Script to the values in the current Master AutoLogin Script Template.

---

### ***Save all current values***

Clicking this button causes all user modifiable fields displayed in this panel to be saved for use by the ANSI Telnet Manager. These are the values that are displayed the next time this named autologin script in the browser tree is selected.

### ***Parameters***

#### ***First Prompt***

This text field allows the user to enter the first string of text to look for in the incoming host data stream. This field is a string with maximum length of 64 characters.

The default value of this field is the value from the AutoLogin Scripts Master Template “First Prompt” field in effect when this named autologin script was created.

#### ***First Response***

This text field indicates the text string that should be sent back to the host when the “First Prompt” string is encountered. This field is a string with maximum length of 64 characters.

Default value for this field is the value from the AutoLogin Scripts Master Template “First Response” field in effect when this named autologin script was created.

#### ***Second Prompt***

This text field allows the user to enter the second string of text to look for in the incoming host data stream. This field is a string with maximum length of 64 characters.

The default value of this field is the value from the AutoLogin Scripts Master Template “Second Prompt” field in effect when this named autologin script was created.

#### ***Second Response***

This text field indicates the text string that should be sent back to the host when the “Second Prompt” string is encountered. This field is a string with maximum length of 64 characters.

Default value for this field is the value from the AutoLogin Scripts Master Template “Second Response” field in effect when this named autologin script was created.

#### ***Third Prompt***

This text field allows the user to enter a third string of text to look for in the incoming host data stream. This field is a string with maximum length of 64 characters.

The default value of this field is the value from the AutoLogin Scripts Master Template “Third Prompt” field in effect when this named autologin script was created.

#### ***Third Response***

This text field indicates the text string that should be sent back to the host when the “Third Prompt” string is encountered. This field is a string with maximum length of 64 characters.

Default value for this field is the value from the AutoLogin Scripts Master Template “Third Response” field in effect when this named autologin script was created.

#### ***Fourth Prompt***

This text field allows the user to enter a fourth string of text to look for in the incoming host data stream. This field is a string with maximum length of 64 characters.

The default value of this field is the value from the AutoLogin Scripts Master Template “Fourth Prompt” field in effect when this named autologin script was created.

#### ***Fourth Response***

This text field indicates the text string that should be sent back to the host when the “Fourth Prompt” string is encountered. This field is a string with maximum length of 64 characters.

Default value for this field is the value from the AutoLogin Scripts Master Template “Fourth Response” field in effect when this named autologin script was created.

---

### ***Fifth Prompt***

This text field allows the user to enter a fifth string of text to look for in the incoming host data stream. This field is a string with maximum length of 64 characters.

The default value of this field is the value from the AutoLogin Scripts Master Template “Fifth Prompt” field in effect when this named autologin script was created.

### ***Fifth Response***

This text field indicates the text string that should be sent back to the host when the “Fifth Prompt” string is encountered. This field is a string with maximum length of 64 characters.

Default value for this field is the value from the AutoLogin Scripts Master Template “Fifth Response” field in effect when this named autologin script was created.

### ***Sixth Prompt***

This text field allows the user to enter a sixth string of text to look for in the incoming host data stream. This field is a string with maximum length of 64 characters.

The default value of this field is the value from the AutoLogin Scripts Master Template “Sixth Prompt” field in effect when this named autologin script was created.

### ***Sixth Response***

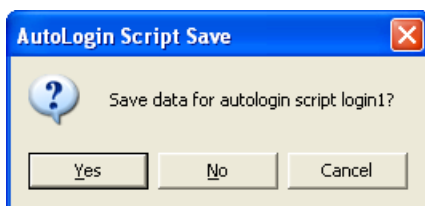
This text field indicates the text string that should be sent back to the host when the “Sixth Prompt” string is encountered. This field is a string with maximum length of 64 characters.

Default value for this field is the value from the AutoLogin Scripts Master Template “Sixth Response” field in effect when this named autologin script was created.

## ***Dialog Boxes / Errors***

### ***AutoLogin Script Save***

If the AutoLogin Scripts named script item in the browser tree loses focus (some other item in the browser tree is selected or the ANSI TM1Config interface is closed), the panel is checked for unsaved changes. If any unsaved changes are detected, a dialog box is displayed to notify the user and request the desired action.



#### ***Select Yes***

All user modifiable fields displayed in the Named AutoLogin Script are saved for use by the ANSI Telnet Manager.

These are the values that are displayed the next time the autologin script is selected from the browser panel. The dialog box is removed from the display.

#### ***Select No***

All user modified values in this panel are discarded and no changes are made.

The most recent previously saved values are displayed the next time this named autologin script item in the browser tree is selected. The dialog box is removed from the display.

#### ***Select Cancel***

Focus is restored to the AutoLogin Scripts item in the browser panel and no changes are made.

None of the field values are altered and the dialog box is removed from the display.

---

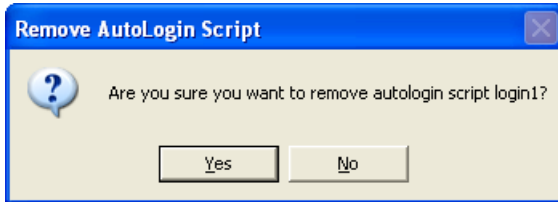
### **Select Close control**

Equivalent to the Cancel button.

### **Removing a Named AutoLogin Script**

Using the mouse right-click function in the browser panel when one of the named autologin script items is highlighted displays an option menu that contains a single choice -- to remove the selected script. The dialog box requests the user for confirmation to remove the selected autologin script.

*Note: If the autologin script is in use by one or more registered client devices, the autologin script cannot be removed.*



#### **Select Yes**

If the specified autologin script is not assigned to a registered client or to the client registration master template, the script is removed. Entries for this autologin script are removed and are no longer available to the ANSI Telnet Manager.

The browser panel is refreshed to show the browser tree without the removed autologin script. The dialog box is removed from the display.

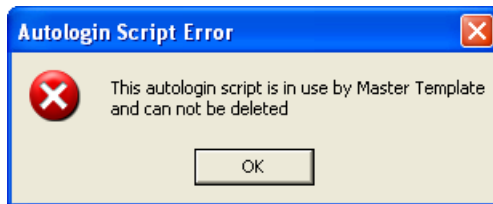
#### **Select No**

The specified autologin script is retained. The dialog box is removed from the display.

### **AutoLogin Script Error**

If the Autologin script being removed is in use by one or more of the registered client devices, or if the client device master template uses it, it cannot be removed. In this case, if the user selects the "Yes" option at the "Remove Login Script" dialog box above, the actions specified above do not occur and a new dialog box is displayed.

If more than one client uses the script, only the first client encountered is listed in the dialog box.



#### **Select OK**

The specified autologin script is retained. The dialog box is removed from the display.

### **Select Close control**

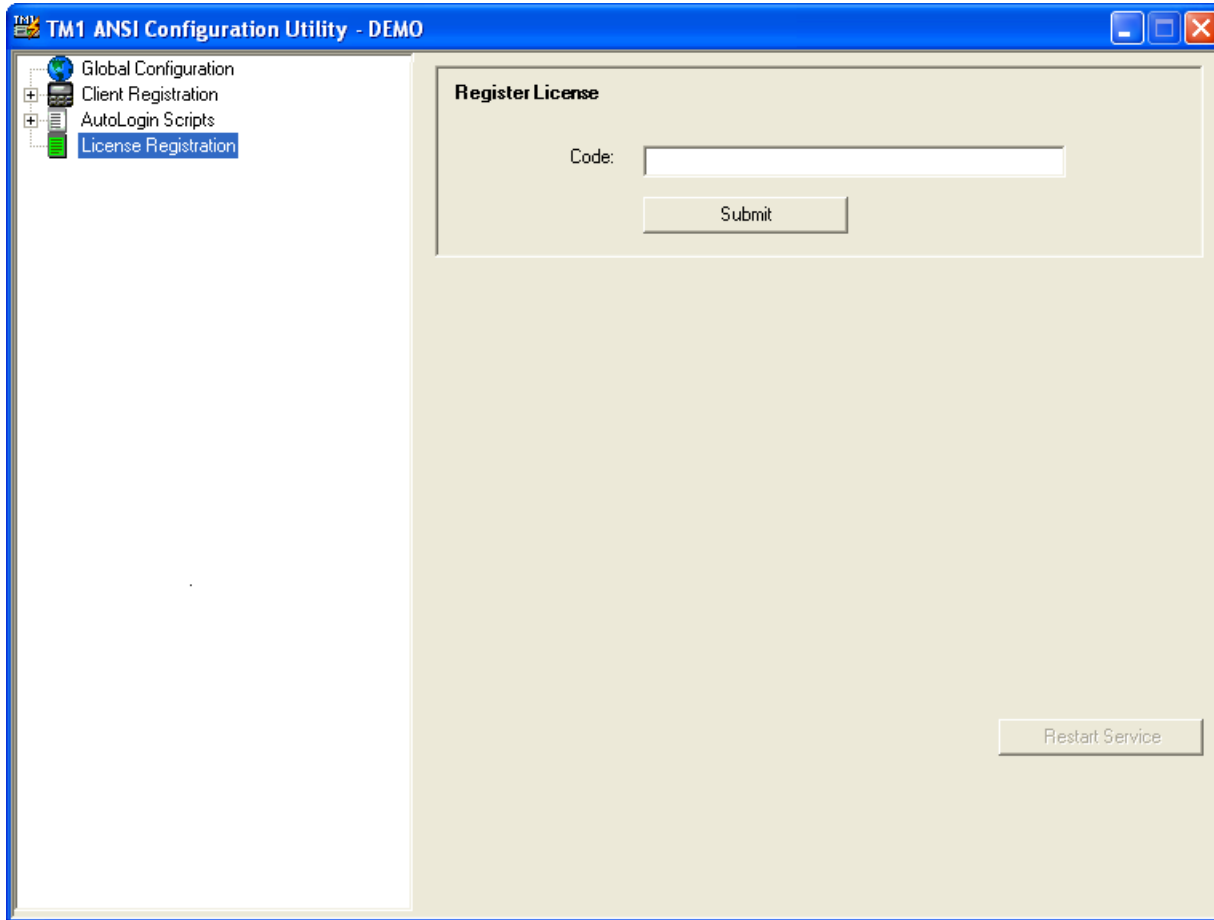
Equivalent to the OK button.

## **License Registration**



The License Registration option is only displayed in the Browser Panel if a valid license key has not previously been entered.

Telnet Manager remains in Demo mode until a valid license key is entered. To enter a license key, click on the License Registration branch.



If Telnet Manager was purchased, a license key was included. Refer to the License Key letter provided for the key. Note that the key is case sensitive.

Contact [Technical Assistance](#) (page 1) with any purchase or license key questions.

When the key is entered, click the submit button to verify the key.

## **Buttons**

### **Submit**

The submit button verifies the license key entered.

If a valid license key is entered, a “success” message is displayed. Telnet Manager is no longer in demo mode.

The DEMO notation in the title bar, the “days remaining” message and the License Registration branch are all removed when TM1Config is next initiated.

If an error message is displayed, double check the key. Remember, the license key is case sensitive. Telnet Manager remains in Demo mode until a valid key is entered.

### **Restart Service**

Clicking this button stops and restarts the TM1 service. If the service is not already running, this button starts the service. This button is not active on this screen until a valid license key is entered.

*Note: Restarting the service terminates any existing client connections.*

## IBM 3270 Configuration Utility

### Introduction

The IBM 3270 TM1Config configuration interface is launched by selecting **Start > Honeywell > Telnet Manager > TM1Config** or double-clicking the TM1Config icon on the desktop. This is the display that is shown first.

The screenshot shows the 'TM1 IBM3270 Configuration Utility' window. On the left, a tree view has 'Global Configuration' selected. The main area contains several configuration sections:

- Terminal Connection:**
  - Allow unregistered terminals to connect
  - Only accept connections via local SSH server
  - Port 1: 4000 Port 2: 4001 Port 3: 4002 Port 4: 4003
- Terminal ID Mode:**
  - MAC Address (SNMP)
  - IP Address (Legacy)
- Radio Server Fast Failover:**
  - Enable
  - Message Port: -1
- TCP/IP Host KeepAlive:**
  - Disable
  - Initial delay in milliseconds: 7200000
  - Retry interval in milliseconds: 75000
- Connection Response Delay:**
  - 250 milliseconds
- SNMP Traps:**
  - Enable
  - Community name: public
  - Host: 10.0.0.1 Port: 162
- Log File:**
  - Disable
  - Limit Maximum Size: 0 MB
  - Limit Maximum Number: 0
  - Directory: C:\Program Files\Honeywell\Telnet Manager\IBM3270\log

At the bottom, there are three buttons: 'Restore factory default values', 'Save current values', and 'Restart Service'.

The Global Configuration branch of the browser tree is highlighted, and all the configurable global parameters (when selected) are displayed in the configuration panel.

### IBM 3270 Telnet Manager Components

#### Global Configuration

This branch contains no leaves. Global parameters are parameters that are independent of the individual client computers. These parameters affect the operation of the session management function, the connection with the host computer or generally apply to all client devices.

#### Client Registration

This branch contains the following leaves:

##### **Client Registration Master Template Parameters**

This leaf defines a template of client registration parameters that are applied by default to new client devices added to the Telnet Manager.

---

## **Client Registration Registered Client Parameters**

There is one of these leaves for each client computer identified to the IBM 3270 Telnet Manager. These leaves are labeled using the identification string associated with the particular client computer. For IBM 3270 session management, the identification string may be the terminal's IP address or the radio MAC address.

### **Registration License**

When Telnet Manager is running in Demo mode, the License Registration branch is displayed. If a valid key has previously been entered, this branch is no longer displayed.

This branch contains no leaves. The registration license key is entered on this screen to switch Telnet Manager from demo to regular mode.

## **IBM 3270 Global Configuration Parameters**

### **Factory Defaults**

Terminal Connection	Allow Unregistered Devices to Connect enabled Only accept connections via local SSH server (applicable only if WinSSHD is installed) Port 1 = 4000, Port 2 = 4001, Port 3 = 4002, Port 4 = 4003
Terminal ID Mode	MAC Address (SNMP)
Radio Server Fast Failover	Disabled. (N/A on IBM3270).
TCP/IP Host KeepAlive	Enabled. Initial delay: 7200000 milliseconds (2 hours) Retry interval: 75000 milliseconds (1.25 minutes)
Connection Response Delay	250 milliseconds
SNMP Traps	Disabled. When enabled: Community Name: 'public' Host: 10.0.0.1 Port: 162
Log File	Log file enabled, no limits on file size or number of log files. Location: <install directory>\3270\LOG i.e.: C:\Program Files\Honeywell\Telnet Manager\3270\log or C:\Program Files (x86)\Honeywell\Telnet Manager\3270\log

### **Buttons**

#### **Restore Values to Factory Default**

Clicking this button causes all user modifiable fields to be restored to the factory default values.

#### **Save current values**

Clicking this button causes all user modifiable fields displayed in this panel to be saved for use by the IBM 3270 Telnet Manager.

These are the values that are displayed the next time the Global Configuration item in the browser tree is selected.

#### **Restart Service**

Clicking this button stops and restarts the TM1 service. If the service is not already running, this button starts the service.

*Note: Restarting the service terminates any existing client connections.*

When configuration data is changed, use the Restart Service button to restart the TM1 service using the changed parameters.



---

## Parameters

### Terminal Connection

#### **Allow Unregistered Terminals to Connect**

Typically, this option is used when setting up a system, for example when finding all client devices while configuring Telnet Manager. Once configured, and all client devices are registered with Telnet Manager, change this setting to not allow unregistered devices.

The checkbox controls the ability of client devices not previously registered with Telnet Manager to connect to Telnet Manager.

When selected, unregistered devices are allowed to connect to the host through the IBM 3270 Telnet Manager. Selecting this checkbox also causes the configuration interface to refresh the browser panel display every ten seconds. This is done to constantly present a relatively current list of all connected client devices.

When not selected, connection attempts by unregistered devices are blocked. In this case, there is no need to refresh the browser panel.

Default is selected – unregistered devices are allowed to connect.

#### **Only Accept Connections via Local SSH Server**

*Note: This setting is applicable only if WinSSHD is installed.*

When selected, only incoming connections through the SSH server are allowed. When this option is selected and the Use SSH Tunnel option is selected on the Master Template, all Telnet Manager connections use SSH from end to end.

When not selected, standard telnet connections are accepted for incoming transmissions. Even if the Use SSH Tunnel option is selected, only the outgoing transmissions use SSH.

Default is selected – only accept connections via SSH server.

#### **Port 1 – 4**

These four text fields allow the user to specify the four TCP/IP ports the IBM 3270 Telnet Manager listens to for client connection attempts.

Fields edits are disabled if the port assigned to the field is in use by any of the defined client profiles.

Fields are validated for a legal port number (an integer in the range 1024 – 65535).

Default values are Port 1 = 4000, Port 2 = 4001, Port 3 = 4002, Port 4 = 4003.

*Note: On Windows XP SP2 or Windows Server 2003, the installation process configures the Windows firewall for Telnet Manager. If you are using a third-party firewall, you must manually open these ports or provide an exception for the Telnet Manager service.*

### Terminal ID Mode

#### **MAC Address (SNMP)**

If this option is selected, IBM 3270 Telnet Manager uses the MAC address to identify the mobile device.

#### **IP Address (Legacy)**

If this option is selected, IBM 3270 Telnet Manager uses the IP address to identify the mobile device. If using legacy (DOS) devices, this option should be enabled.

### Radio Server Fast Failover

Radio server fast failover is not supported on the IBM 3270 Telnet Manager.

### TCP/IP Host KeepAlive

The TCP/IP Host KeepAlive function prevents the TCP/IP socket connection between the application host and Telnet Manager from being torn down if the host is present. In a situation where there is no traffic between the host and Telnet Manager for a long time, Telnet Manager sends a KeepAlive message to the host computer. If the host responds, Telnet Manager knows the host is still present and keeps the socket open. If the host does not respond to repeated Keep-

---

Alive messages, Telnet Manager closes the socket to the host. This disables communications between the host and Telnet Manager until a new socket is negotiated. If Telnet Manager closes the host socket, it also closes the socket opened to the client computer as well. (With no host, there is no point in keeping the client connected.)

The Host KeepAlive function plays a role only if there has been no activity on the Telnet Manager / host link for a period of time. The Host KeepAlive timer is reset on every message received from the host computer. The Host KeepAlive function is useful to detect a failure on the host communications link during periods of inactivity. If the host connection is lost and Telnet Manager closes the socket, it also issues a Host KeepAlive SNMP Trap message.

Telnet session 'keep-alive' is controlled by three parameters:

**Initial delay in milliseconds:** This is the length of time of no activity from the host before sending the KeepAlive message.

**Retry Interval in milliseconds:** The length of time between KeepAlive message retries.

**Disable Host KeepAlive:** This parameter enables or disables the telnet session 'keep-alive' functionality.

### ***Disable***

This checkbox governs the host KeepAlive behavior of the IBM 3270 Telnet Manager.

If the Host KeepAlive function is disabled, Telnet Manager does not send KeepAlive messages to the host computer, and does not close the socket to the host during periods of inactivity on the link.

When checked, the host KeepAlive is disabled. When checked, this control causes other data entry fields in this section to be disabled.

### ***Initial delay in milliseconds***

This text field indicates the duration of inactivity on the host link that Telnet Manager waits before sending a KeepAlive message to the host. The value is specified in milliseconds, and is validated for an integer number in the range 300,000 – 7,200,000.

Default value for this field is 7200000 milliseconds (2 hours).

### ***Retry interval in milliseconds***

This text field indicates the time to wait before sending another Host KeepAlive message if the host has not responded to the previous KeepAlive message(s). The host socket is closed, and a Host KeepAlive SNMP trap is issued, if the host does not respond to 5 consecutive KeepAlive messages. The value of the "Retry interval in milliseconds" field is specified in milliseconds, and is validated for an integer number in the range 10,000 – 75,000.

Default value for this field is 75000 milliseconds (1.25 minutes).

### ***Connection Response Delay***

Provides a delay between when the computer connects to the Telnet Manager and when Telnet Manager issues the request for the LU# from the computer.

The value of the "Connection response delay" field is specified in milliseconds, and is validated for an integer number in the range 1 – 2,000.

Default value for this field is 250 milliseconds.

### ***SNMP Traps***

SNMP Traps are logged for the following actions:

Application host communications failure. An alarm event Trap is generated if Telnet Manager loses communications with any host for which a session is currently open.

Terminal communications failure. Telnet Manager generates an alarm event if a specific client device is disconnected due to a 'keep-alive' time out more than a specified number of times.

Telnet Manager Boot. When Telnet Manager goes through a Boot for whatever reason a "Boot Trap" is sent.

### ***Enable***

This checkbox controls the Telnet Manager SNMP Trap function.

---

When checked, Telnet Manager sends traps to the Trap Destination IP address (see below). When deselected, Telnet Manager does not send SNMP traps. When deselected, this control causes other data entry fields in this section to be disabled.

The default value for this checkbox is deselected.

### **Community Name**

This text field indicates the SNMP community name. This field is validated for a string with a maximum length of 32 characters.

Default value for this field is 'public'.

### **Host**

This text field indicates the IP address or Domain Name of the network manager that is to receive SNMP trap messages generated by the IBM 3270 Telnet Manager. This field is NOT validated for correct IP address format (1.0.0.0 to 254.254.254.254).

Default value for this field is 10.0.0.1.

### **Port**

This text field indicates the IP port number on the network manager station to receive SNMP trap messages. This field is validated for a legal port number (an integer in the range 1 – 65535).

Default value for this field is 162.

## **Log File**

### **Disable**

When checked, no log file is kept.

The default is unchecked – a log file is maintained by Telnet Manager.

### **Limit Maximum Size**

This option determines the maximum file size (in MB) that Telnet Manager maintains for the log file. Once the maximum size is reached, Telnet Manager starts a new log file.

The default is unchecked – no limit on log file size.

To enable, check the box and specify a maximum file size in MB in the text box.

### **Limit Maximum Number**

This option determines the maximum number of log files that can accumulate before deleting the oldest log file. A new log file is created when either of the following occurs:

- The maximum file size is reached (see the parameter above)
- The Telnet Manager service is restarted.

The default is unchecked – no limit on the number of log files maintained.

To enable, check the box and specify the number of log files to keep.

### **Directory**

This text parameter holds the name of the directory path for the IBM 3270 Telnet Manager log file.

Default value for this field is <install directory>\3270\LOG (when installed in the default directory, C:\Program Files\Honeywell\Telnet Manager\3270\log or C:\Program Files (x86)\Honeywell\Telnet Manager\3270\log).

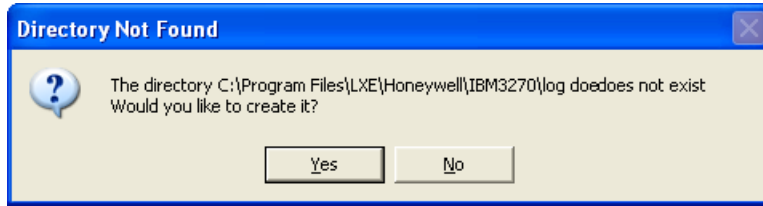
This field is validated to ensure the directory already exists.

The Browse button can be used to select a location for the log file.

## **Dialog / Error Boxes**

### **Directory Does Not Exist**

If the debug log file directory does not exist when the 'Save Current Values' button is clicked, a dialog box alerts the user and asks if the directory is to be created.



### **Select Yes**

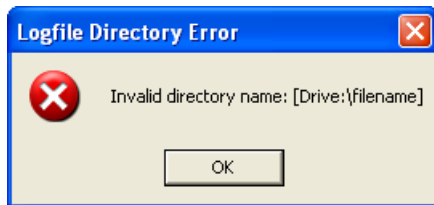
The directory specified in the Debug Log File Directory location is created and the dialog box is removed from the display.

### **Select No**

The directory specified in the Debug Log File Directory location control is not changed from the previously saved value. The dialog box is removed from the display.

### **Logfile Directory Error**

If the debug log file directory specified when the 'Save All Current Values' button is selected is not formatted as a valid directory string, a dialog box reminds the user of the format for a valid directory path.



### **Select OK**

The directory specified for the Debug Log File Directory location control is not changed from the previously saved value. The dialog box is removed from the display.

### **Select Close control**

Equivalent to the OK button.

### **Parameter Change Notification**

When the new Global Configuration parameters have been saved, a dialog box appears that states the new parameters do not take effect until Telnet Manager is restarted.



### **Select OK**

The dialog box is removed from the display.

### **Select Close control**

Equivalent to the OK button.

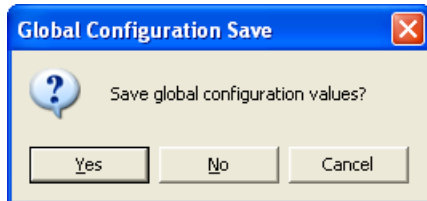
After dismissing the notification, to restart Tm1Service, click the Restart Service button on the Global Configuration screen. For more information on Tm1Service, including alternative methods of restarting the service, see [TM1 Service](#) (page 29).

*Note: Restarting the service terminates any existing client connections.*

---

## **Global Configuration Save**

If the Global Configuration item in the browser tree loses focus (some other item in the browser tree is selected or the IBM 3270 TM1Config interface is closed), the panel is checked for unsaved changes. If any unsaved changes are detected, a dialog box is displayed to notify the user and request the desired action.



### **Select Yes**

All user modifiable fields displayed in this panel are saved for use by the IBM 3270 Telnet Manager. These are the values that are displayed the next time the Global Configuration item in the browser tree is selected. The dialog box is removed from the display.

### **Select No**

The current session's user modified values in this panel are discarded and no changes are made. The previously saved values are displayed the next time the Global Configuration item in the browser tree is selected. The dialog box is removed from the display.

### **Select Cancel**

Focus is restored to the Global Configuration item in the browser panel and no changes are made.

None of the field values are altered and the dialog box is removed from the display.

### **Select Close control**

Equivalent to the Cancel button.

## **IBM 3270 Client Registration**

Selecting the Client Registration item in the browser panel causes no action other than to highlight the Client Registration text and icon in the browser panel.

Selecting this choice causes the "Register a Terminal" interface to be displayed in the Register a terminal panel to appear.

## Registering New Client Devices

The screenshot shows a window titled "TM1 IBM3270 Configuration Utility" with a sidebar containing "Global Configuration" and "Client Registration". The main area is titled "Register a terminal" and contains two input fields: "Terminal identification:" (a text box) and "Terminal incoming connection port:" (a dropdown menu showing "4000"). Below these fields is an "Add New" button.

### Factory Defaults

Terminal Identification	Blank
Terminal incoming connection port	Value assigned to Port 1 in the Global Configuration panel.

### Buttons

#### Add New

Clicking this button causes the specified client identification string and port number to be added to the IBM 3270 Telnet Manager database and the browser panel display is refreshed to include the newly defined client device.

Newly registered client devices are assigned configuration parameters from the Client Registration Master Template in effect at the time the device is registered. If the Terminal Identification field is blank, there is no action.

### Parameters

#### Terminal Identification

This text field stores the text string used to identify the new client device.

This field is validated to conform to a format consistent with the Terminal ID Mode selection on the Global Configuration screen.

- If MAC Address (SNMP) is selected, this field must be a text string formatted as a MAC address. MAC address format is six hexadecimal numbers in the range 0 through ff. Colon characters must separate the six numbers. They may be padded with leading zeros, but that is not required. MAC addresses are NOT case sensitive.

- If IP Address (Legacy) is selected, this field must conform to IP address formatting standards. The octets of the IP address must NOT be padded with leading zeros.

The default value of this field is blank.

### **Terminal Incoming Connection Port**

Select a port from the drop down list. Input is restricted to selecting from the pull-down list. If the value you need does not exist in the pull-down list, it must be added using the Global Configuration panel.

The default value of this field is the value assigned to Port 1 in the Global Configuration panel.

## **Client Registration / Master Template**

Selecting the 'Master Template' item in the browser panel list that is subordinate to Client Registration displays the Terminal Master Template interface in the configuration panel.

Using the mouse right-click function on the 'Master Template' item in the browser panel causes no action.

The screenshot shows the 'TM1 IBM3270 Configuration Utility' window. On the left is a tree view with 'Global Configuration', 'Client Registration', and 'Master Template' (selected). The main area is titled 'Master Template' and contains the following configuration sections:

- Host Connection**
  - Name: 10.0.0.1
  - Port: 23
  - Connection timeout (seconds): 10
  - Connection Management: Always maintain connection (default)
- Ssh**
  - Off (selected), Shell, Tunnel
  - Select Profile: [dropdown]
  - Edit/Create Profile button
- Activity Timeout**
  - Enable checkbox (unchecked)
  - Timeout (minutes): 5
- TCP/IP Terminal KeepAlive**
  - Disable checkbox (unchecked)
  - Initial delay (ms): 7200000
  - Retry interval (ms): 75000

At the bottom are two buttons: 'Restore factory default values' and 'Save current values'.

---

## Factory Defaults

Host Connection	Name: 10.0.0.1 Port: 23 Connection timeout in seconds: 10 seconds Connection Management: Always maintain connection
SSH	Off: Selected (SSH is disabled) Shell: Not Available Tunnel: Unselected Select Profile : N/A
Activity Timeout	Enable: Disabled Timeout (minutes): 5
TCP/IP Terminal KeepAlive	Disable: Enable Initial delay (ms): 7200000 milliseconds (2 hours) Retry interval (ms): 75000 milliseconds (1.25 minutes)

## Buttons

### **Edit/Create Profile**

This button is active only if SSH Tunnel or SSH Shell is selected. When active, this button accesses the [SSH Settings](#) (page 109) screen.

### **Restore Values to Factory Default**

Clicking this button causes all user modifiable fields to be restored to the factory default values.

### **Save current values**

Clicking this button causes all user modifiable fields displayed in this panel to be saved for use by the IBM 3270 Telnet Manager.

These are the values that are displayed the next time the Client Registration / Master Template item in the browser tree is selected.

Values in the Master Template are automatically propagated to the registered terminals. All configuration items for all registered terminals that have not been changed from the Master Template values are immediately updated to reflect the new Master Template configuration.

*Note: Configuration values for registered terminals that have been changed from the Master Template value are not affected.*

## Parameters

In some cases, system administrators are concerned about having client devices logged in but inactive. In these cases, Telnet Manager provides the ability to log the client device off the host if there has been no user activity for a specified time period. The parameters used to manage RF client devices are Host Connection, Manage Terminal Session, and Activity Timeout.

### **Host Connection**

#### **Name**

Enter the IP address or Domain Name of the host computer to which this client device connects into this text field. This field is validated for correct IP address format (1.0.0.0 to 254.254.254.254).

The default value of this field is 10.0.0.1.

*Note: If Use SSH Tunnel (see below) is selected this field is set to 127.0.0.1 and cannot be edited as long as the SSH option is enabled.*



---

## **Port**

This text field indicates the IP port number on the application host to which this client connects. This field is validated for a legal port number (an integer number in the range 1 – 65535).

Default value for this field is 23.

*Note: If Use SSH Tunnel (see below) is selected, the value in this field must be set to the listening port specified in the SSH profile.*

## **Connection Timeout (seconds)**

Enter the host connection timeout value in this text field. This field is validated for an integer in the range 5 – 65535.

Default value for this field is 10.

## **Connection Management**

Use this option to determine the type of Host Connection Management:

- Always close connection
- Always maintain connection (default)
- Close connection on explicit close.

## **SSH**

### **Off**

Telnet is used without SSH.

### **Shell**

This option is not available for IBM 3270.

### **Tunnel**

A connection is established to an SSH server and Telnet traffic is tunneled (port forwarded) through the SSH connection.

*Note: This checkbox can only be accessed if the Include SSH option was selected during installation. Uninstall Telnet Manager and reinstall with the Include SSH option selected to enable this feature.*

## **Select Profile**

Select the name of a previously created SSH connection profile to use. If no profiles exist or to modify an existing

## **Activity Timeout**

The Activity Timeout allows the administrator to logoff a client computer that has been idle for a specified period of time. The client computer is logged off, and a Session Disconnect Activity timeout SNMP Trap is issued, regardless of whether or not the client computer is present on the network. Telnet Manager closes both the socket to the client computer and to the host computer. If this client computer subsequently reconnects to Telnet Manager, it is assigned to a new host session.

### **Enable**

Selecting this checkbox enables the activity timeout feature for this client device. If this checkbox is cleared, data entry in the Timeout in Minutes field is disabled.

The default state of this checkbox is not selected.

### **Timeout (minutes)**

This text field is used to enter the activity timeout value for this client device. This field is validated for an integer in the range 5 – 65535.

If the Enable checkbox is not selected, data entry in this field is disabled.

Default value for this field is 5.

---

## **TCP/IP Terminal KeepAlive**

The TCP/IP Terminal KeepAlive function prevents the TCP/IP socket connection between the individual client computer and Telnet Manager from being torn down if the client computer is present. In a situation where there is no traffic between the client computer and Telnet Manager for a long time, Telnet Manager sends a KeepAlive message to the client. If the client responds, Telnet Manager knows the client is still present and keeps the socket open. If the client computer does not respond to repeated KeepAlive messages, Telnet Manager closes the socket to the client computer. This disables communications between this particular client computer and Telnet Manager until a new socket is negotiated.

The Terminal KeepAlive function plays a role only if there has been no activity on the Telnet Manager / client computer link for a period of time. The Terminal KeepAlive timer is reset on every message received from the client computer. The Terminal KeepAlive function is useful to close unused client computer sockets. If the client computer connection is lost and Telnet Manager closes the socket, it also issues a TE Disconnect SNMP Trap message.

Note that if Telnet Manager closes the client computer socket because the client does not respond to TCP/IP KeepAlive messages, it does not close the corresponding socket to the host computer. If the same client computer reconnects later, it is reconnected to the same host socket – that is, it is reconnected to the same session it had before.

### **Disable**

This control governs the terminal KeepAlive behavior of the IBM 3270 Telnet Manager.

When selected, terminal KeepAlive is disabled and causes the other data entry fields in this section to be disabled. If the Terminal KeepAlive function is disabled, Telnet Manager does not send KeepAlive messages to the client computer, and does not close the socket to the client during periods of inactivity on the link.

When cleared, terminal KeepAlive is enabled.

The default value for this checkbox is cleared.

### **Initial delay (ms)**

This text field indicates the duration of inactivity on the client computer link that Telnet Manager waits before sending a KeepAlive message to the client. The value is specified in milliseconds, and is validated for an integer number in the range 300,000 – 7,200,000.

Default value for this field is 7200000 milliseconds (2 hours).

### **Retry interval (ms)**

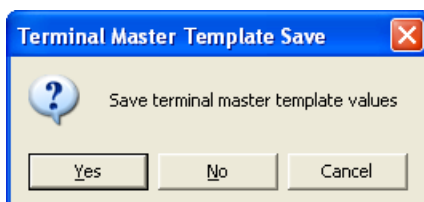
This text field indicates the time to wait before sending another Terminal KeepAlive message if the client computer has not responded to the previous KeepAlive message(s). The client socket is closed, and a TE Disconnect SNMP trap is issued, if the client does not respond to 5 consecutive KeepAlive messages. The value of the “Retry interval in milliseconds” field is specified in milliseconds, and is validated for an integer number in the range 10,000 – 75,000.

Default value for this field is 75000 milliseconds (1.25 minutes).

## **Dialog / Error Boxes**

### **Terminal Master Template Save**

If the Client Registration Master Template item in the browser tree loses focus (some other item in the browser tree is selected or the IBM 3270 TM1Config interface is closed), the panel is checked for unsaved changes. If any unsaved changes are detected, a dialog box is displayed to notify the user and request the desired action.



---

### **Select Yes**

All user modifiable fields displayed in this panel are saved for use by the IBM 3270 Telnet Manager. These are the values that are displayed the next time the Client Registration Master Template item in the browser tree is selected. The dialog box is removed from the display.

### **Select No**

The current session's user modified values in this panel are discarded and no changes are made. The previously saved values are displayed the next time the Client Registration Master Template item in the browser tree is selected. The dialog box is removed from the display.

### **Select Cancel**

Focus is restored to the Client Registration Master Template item in the browser panel and no changes are made.

None of the field values are altered and the dialog box is removed from the display.

### **Select Close control**

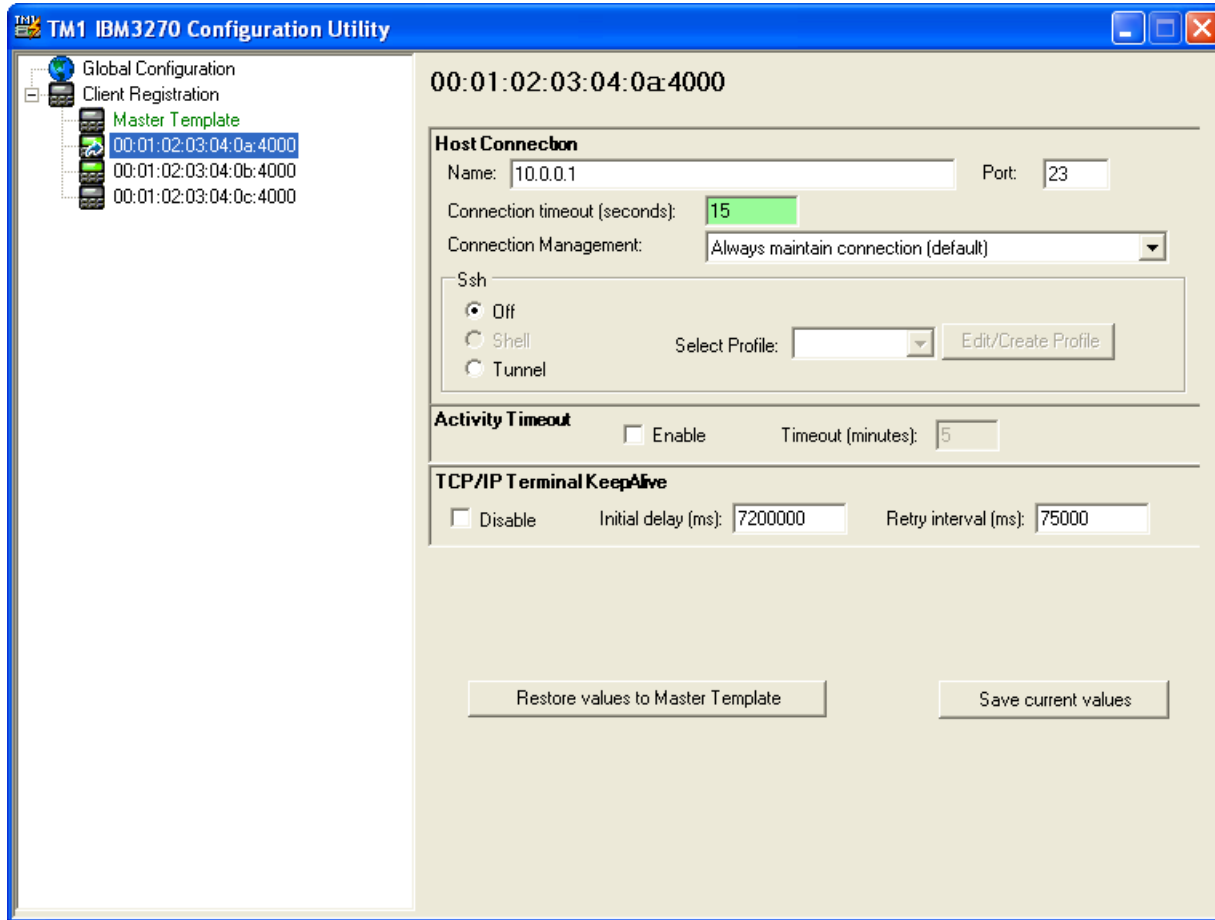
Equivalent to the Cancel button.

## **Client Registration / Registered Clients**

Selecting any of the individual client ID items in the browser panel list that is subordinate to Client Registration displays the Registered Terminal interface in the configuration panel.

If any of the configurable parameters in this configuration panel display differ from the corresponding parameters in the Master Template configuration panel, those controls are highlighted. Likewise the Registered Client icon is also highlighted for any clients whose saved values differ from the Master Template values.

A right mouse click on the selected individual client ID item, displays a one-line menu item – to delete the highlight registered client. Refer to [Removing a Registered Client](#) (page 85) for instruction.



### Factory Defaults

Host Connection	Name: Host Connection IP address of the host computer from the Master Template. Port: Host Connection Port value from the Master Template. Connection timeout in seconds: Host Connection Timeout value From the Master Template. Connection Management: Value from the Master Template.
SSH	Off, Tunnel: Value from the Master Template Select Profile: Value from the Master Template
Activity Timeout	Enable: Activity Timeout Enable checkbox from the Master Template. Timeout (minutes): Activity Timeout / Timeout in Minutes value from the Master Template.
TCP/IP Terminal KeepAlive	Disable: Disable checkbox status from the Master Template. Initial delay (ms): TCP/IP Terminal KeepAlive / Initial delay in milliseconds value from the Master Template. Retry interval (ms): TCP/IP Terminal KeepAlive / Retry interval in milliseconds value from the Master Template.

### Buttons

#### **Edit/Create Profile**

This button is active only if SSH Tunnel or SSH Shell is selected. When active, this button accesses the [SSH Settings](#) (page 109) screen.

---

### **Restore Values to Master Template**

Clicking this button causes all user modifiable fields to be restored to the values defined by the current Client Configuration Master Template.

### **Save current values**

Clicking this button causes all user modifiable fields displayed in this panel to be saved for use by the IBM 3270 Telnet Manager.

These are the values that are displayed the next time this Client ID is selected in the Client Registration branch of the browser tree.

### **Parameters**

In some cases, system administrators are concerned about having client devices logged in but inactive. In these cases, Telnet Manager provides the ability to log the client device off the host if there has been no user activity for a specified time period. The parameters used to manage RF client devices are Host Connection, Manage Terminal Sessions, and Activity Timeout.

#### **Host Connection**

##### **Name**

Enter the IP address or Domain Name of the host computer to which this client device connects into this text field. This field is validated for correct IP address format (1.0.0.0 to 254.254.254.254).

The default value of this field is the Host Connection IP Address value from the Master Template.

##### **Port**

This text field indicates the IP port number on the application host to which this client connects. This field is validated for a legal port number (an integer number in the range 1 – 65535).

Default value for this field is the Host Connection Port value from the Master Template.

*Note: If Use SSH Tunnel (see below) is selected, the value in this field must be set to the listening port specified in the SSH profile.*

##### **Connection Timeout (seconds)**

Enter the host connection timeout value in this text field. This field is validated for an integer in the range 5 – 65535.

Default value for this field is the Host Connection Timeout in Seconds value from the Master Template.

##### **Connection Management**

Use this option to determine the type of Connection Management:

- Always close connection
- Always maintain connection (default)
- Close connection on explicit close.

##### **SSH**

Default value for SSH is the connection type from the Master Template.

##### **Off**

Telnet is used without SSH.

##### **Shell**

This option is not available for IBM 3270.

##### **Tunnel**

A connection is established to an SSH server and Telnet traffic is tunneled (port forwarded) through the

---

SSH connection.

*Note: If this option is enabled on the Client Registration Master Template, the default SSH tunnel is created at TM1 startup. If a different SSH tunnel connection profile is used for a registered terminal, there may be a delay when first connecting as it can take up to 20 seconds to establish an SSH tunnel.*

### **Select Profile**

Select the name of a previously created SSH connection profile to use. If no profiles exist or to modify an existing profile, use the **Edit/Create Profile** button to access the [SSH Settings](#) (page 109) screen.

The default value is the profile (if any) from the Master Template.

### **Activity Timeout**

#### **Enable**

Selecting this checkbox enables the activity timeout feature for this client device. If this checkbox is cleared, data entry in the Timeout in Minutes field is disabled.

Default state for this checkbox is the state of the Activity Timeout Disable checkbox from the Master Template.

#### **Timeout (minutes)**

This text field is used to enter the activity timeout value for this client device. This field is validated for an integer in the range 5 – 65535.

Default value for this field is the Activity Timeout / Timeout in Minutes value from the Master Template.

### **TCP/IP Terminal KeepAlive**

The TCP/IP Terminal KeepAlive function prevents the TCP/IP socket connection between the individual client computer and Telnet Manager from being torn down if the client computer is present. In a situation where there is no traffic between the client computer and Telnet Manager for a long time, Telnet Manager sends a KeepAlive message to the client. If the client responds, Telnet Manager knows the client is still present and keeps the socket open. If the client computer does not respond to repeated KeepAlive messages, Telnet Manager closes the socket to the client computer. This disables communications between this particular client computer and Telnet Manager until a new socket is negotiated.

The Terminal KeepAlive function plays a role only if there has been no activity on the Telnet Manager / client computer link for a period of time. The Terminal KeepAlive timer is reset on every message received from the client computer. The Terminal KeepAlive function is useful to close unused client computer sockets. If the client computer connection is lost and Telnet Manager closes the socket, it also issues a TE Disconnect SNMP Trap message.

Note that if Telnet Manager closes the client computer socket because the client does not respond to TCP/IP KeepAlive messages, it does not close the corresponding socket to the host computer. If the same client computer reconnects later, it is reconnected to the same host socket – that is, it is reconnected to the same session it had before.

#### **Disable**

This control governs the terminal KeepAlive behavior of the IBM 3270 Telnet Manager.

When selected, terminal KeepAlive is disabled and causes the other data entry fields in this section to be disabled. If the Terminal KeepAlive function is disabled, Telnet Manager does not send KeepAlive messages to the client computer, and does not close the socket to the client during periods of inactivity on the link.

When cleared, terminal KeepAlive is enabled.

The default value for this field is the Disable checkbox status from the Master Template.

#### **Initial delay (ms)**

This text field indicates the duration of inactivity on the client computer link that Telnet Manager waits before sending a KeepAlive message to the client. The value is specified in milliseconds, and is validated for an integer number in the range 300,000 – 7,200,000.

---

Default value for this field is the TCP/IP Terminal KeepAlive / Initial delay in milliseconds value from the Master Template or 7200000 milliseconds (2 hours).

### **Retry interval (ms)**

This text field indicates the time to wait before sending another Terminal KeepAlive message if the client computer has not responded to the previous KeepAlive message(s). The client socket is closed, and a TE Disconnect SNMP trap is issued, if the client does not respond to five consecutive KeepAlive messages.

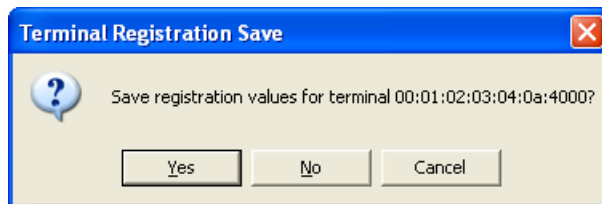
The value of this field is specified in milliseconds, and is validated for an integer number in the range 10,000 – 75,000.

Default value for this field is the TCP/IP Terminal KeepAlive / Retry interval in milliseconds value from the Master Template.

## **Dialog / Error Boxes**

### **Terminal Registration Save**

If the Client Registration individual client ID item in the browser tree loses focus (some other item in the browser tree is selected or the IBM 3270 Telnet Manager configuration interface is closed), the panel is checked for unsaved changes. If any unsaved changes are detected, a dialog box is displayed to notify the user and request the desired action.



#### **Select Yes**

All user modifiable fields displayed in this panel are saved for use by the IBM 3270 Telnet Manager. These are the values that are displayed the next time this individual client ID item in the browser tree is selected. The dialog box is removed from the display.

#### **Select No**

The current session's user modified values in this panel are discarded and no changes are made. The previously saved values are displayed the next time this individual client ID is selected. The dialog box is removed from the display.

#### **Select Cancel**

Focus is restored to the Client Registration Master Template in the browser panel and no changes are made. None of the field values are altered and the dialog box is removed from the display.

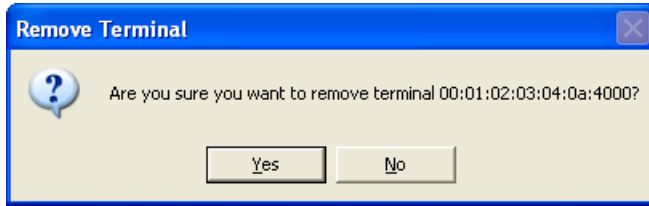
#### **Select Close control**

Equivalent to the Cancel button.

### **Removing a Registered Client**

Using the mouse right-click function in the browser panel when one of the individual client ID items has focus (is highlighted) causes an option menu to be displayed.

The option menu contains the single choice to remove the selected client. Selecting this choice causes the "Remove Terminal" dialog box to be displayed. The dialog box requests the user for confirmation to remove the selected terminal registration. The individual client ID text and icon retain their highlighted (selected) status until the removal is confirmed.



### **Select Yes**

Selecting this option causes the specified terminal registration to be removed and entries for this terminal are removed and are no longer available to the IBM 3270 Telnet Manager. The browser panel is refreshed to show the browser tree without the removed terminal. Focus in the browser panel shifts to the terminal that previously followed the removed terminal.

If the removed terminal was the last terminal in the list, focus shifts to the preceding terminal in the list. If the removed terminal was the only terminal in the list, focus shifts to the Client Registration Master Template

The configuration panel is refreshed to reflect the item now selected in the browser panel and the Remove Terminal dialog box is removed from the display.

### **Select No**

The specified terminal registration is retained and the Remove Terminal dialog box is removed from the display.

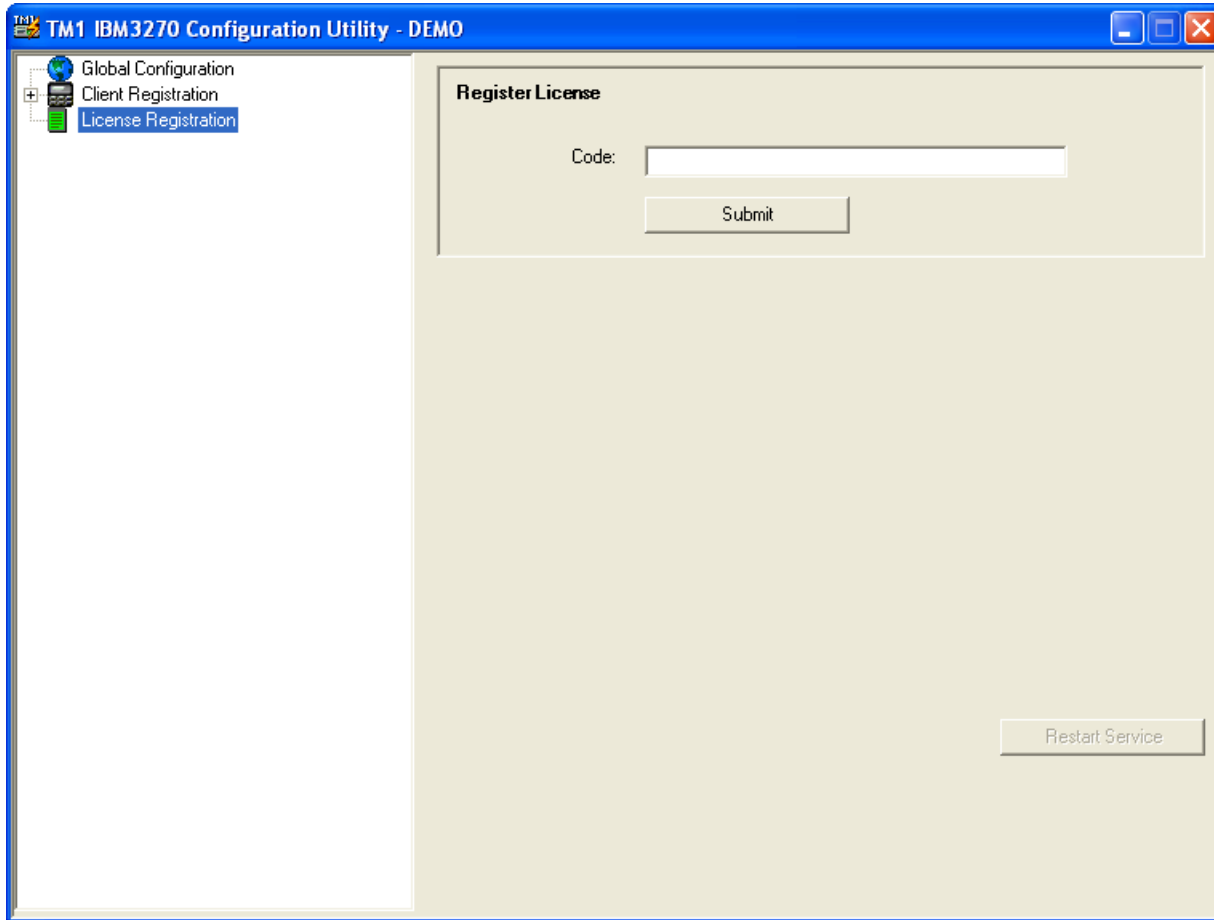
## **License Registration**



The License Registration option is only displayed in the Browser Panel if a valid license key has not previously been entered.

Telnet Manager remains in Demo mode until a valid license key is entered. To enter a license key, click on the License Registration branch.





If Telnet Manager was purchased, a license key was included. Refer to the License Key letter provided for the key. Note that the key is case sensitive.

Contact [Technical Assistance](#) (page 1) with any purchase or license key questions.

When the key is entered, click the submit button to verify the key.

## **Buttons**

### **Submit**

The submit button verifies the license key entered.

If a valid license key is entered, a “success” message is displayed. Telnet Manager is no longer in demo mode.

The DEMO notation in the title bar, the “days remaining” message and the License Registration branch are all removed when TM1Config is next initiated.

If an error message is displayed, double check the key. Remember, the license key is case sensitive. Telnet Manager remains in Demo mode until a valid key is entered.

### **Restart Service**

Clicking this button stops and restarts the TM1 service. If the service is not already running, this button starts the service. This button is not active on this screen until a valid license key is entered.

*Note: Restarting the service terminates any existing client connections.*



## IBM 5250 Configuration Utility

### Introduction

The IBM 5250 TM1Config configuration interface is launched by selecting **Start > Honeywell > Telnet Manager > TM1Config** or double-clicking the TM1Config icon on the desktop. This is the display that is shown first.

The screenshot shows the 'TM1 IBM5250 Configuration Utility' window. On the left, a tree view has 'Global Configuration' selected. The main panel displays several configuration sections:

- Terminal Connection:**
  - Allow unregistered terminals to connect
  - Only accept connections via local SSH server
  - Port 1: 4000, Port 2: 4001, Port 3: 4002, Port 4: 4003
- Terminal ID Mode:**
  - MAC Address (SNMP)
  - IP Address (Legacy)
- Radio Server Fast Failover:**
  - Enable
  - Message Port: -1
- TCP/IP Host KeepAlive:**
  - Disable
  - Initial delay in milliseconds: 7200000
  - Retry interval in milliseconds: 75000
- Connection Response Delay:**
  - 250 milliseconds
- SNMP Traps:**
  - Enable
  - Community name: public
  - Host: 10.0.0.1, Port: 162
- Log File:**
  - Disable
  - Limit Maximum Size: 0 MB
  - Limit Maximum Number: 0
  - Directory: C:\Program Files\Honeywell\Telnet Manager\IBM3270\log

At the bottom, there are three buttons: 'Restore factory default values', 'Save current values', and 'Restart Service'.

The Global Configuration branch of the browser tree is highlighted, and all the configurable global parameters (when selected) are displayed in the configuration panel.

### IBM 5250 Telnet Manager Components

#### Global Configuration

This branch contains no leaves. Global parameters are parameters that are independent of the individual client computers. These parameters affect the operation of the Telnet Manager application, the connection with the host computer or generally apply to all client devices.

#### Client Registration

This branch contains the following leaves:

##### Client Registration Master Template Parameters

This leaf defines a template of client registration parameters that are applied by default to new client devices added to the Telnet Manager.

---

## **Client Registration Registered Client Parameters**

There is one of these leaves for each client computer identified to the IBM 5250 Telnet Manager. These leaves are labeled using the identification string associated with the particular client computer. For IBM 5250 session management, the identification string may be either the terminal's IP address or the radio MAC address.

### **Registration License**

When Telnet Manager is running in Demo mode, the License Registration branch is displayed. If a valid key has previously been entered, this branch is no longer displayed.

This branch contains no leaves. The registration license key is entered on this screen to switch Telnet Manager from demo to regular mode.

## **IBM 5250 Global Configuration Parameters**

### **Factory Defaults**

Terminal Connection	Allow Unregistered Devices to Connect enabled Only accept connections via local SSH server (applicable only if WinSSHD is installed) Port 1 = 4000, Port 2 = 4001, Port 3 = 4002, Port 4 = 4003
Terminal ID Mode	MAC Address (SNMP)
Radio Server Fast Failover	Disabled. (N/A on IBM5250).
TCP/IP Host KeepAlive	Enabled. Initial delay: 7200000 milliseconds (2 hours) Retry interval: 75000 milliseconds (1.25 minutes)
Connection Response Delay	250 milliseconds
SNMP Traps	Disabled. When enabled: Community Name: 'public' Host: 10.0.0.1 Port: 162
Log File	Log file enabled, no limits on file size or number of log files Location: <install directory>\5250\log i.e.: C:\Program Files\Honeywell\Telnet Manager\5250\log or C:\Program Files (x86)\Honeywell\Telnet Manager\5250\log

### **Buttons**

#### **Restore Values to Factory Default**

Clicking this button causes all user modifiable fields to be restored to the factory default values.

#### **Save current values**

Clicking this button causes all user modifiable fields displayed in this panel to be saved for use by the IBM 5250 Telnet Manager.

These are the values that are displayed the next time the Global Configuration item in the browser tree is selected.

#### **Restart Service**

Clicking this button stops and restarts the TM1 service. If the service is not already running, this button starts the service.

*Note: Restarting the service terminates any existing client connections.*

When configuration data is changed, use the Restart Service button to restart the TM1 service using the changed parameters.

---

## Parameters

### Terminal Connection

#### **Allow Unregistered Terminals to Connect**

Typically, this option is used when setting up a system, for example when finding all client devices while configuring Telnet Manager. Once configured, and all client devices are registered with Telnet Manager, change this setting to not allow unregistered devices.

The checkbox controls the ability of client devices not previously registered with Telnet Manager to connect to Telnet Manager.

When selected, unregistered devices are allowed to connect to the host through the IBM 5250 Telnet Manager. Selecting this checkbox also causes the configuration interface to refresh the browser panel display every ten seconds. This is done to constantly present a relatively current list of all connected client devices.

When not selected, connection attempts by unregistered devices are blocked. In this case, there is no need to refresh the browser panel.

Default is selected – unregistered devices are allowed to connect.

#### **Only Accept Connections via Local SSH Server**

*Note: This setting is applicable only if WinSSHD is installed.*

When selected, only incoming connections through the SSH server are allowed. When this option is selected and the Use SSH Tunnel option is selected on the Master Template, all Telnet Manager connections use SSH from end to end.

When not selected, standard telnet connections are accepted for incoming transmissions. Even if the Use SSH Tunnel option is selected, only the outgoing transmissions use SSH.

Default is selected – only accept connections via SSH server.

#### **Port 1 – 4**

These four text fields allow the user to specify the four TCP/IP ports the IBM 5250 Telnet Manager listens to for client connection attempts.

Fields are disabled if the port assigned to the field is in use by any of the defined client profiles.

Fields are validated for a legal port number (an integer in the range 1024 – 65535).

Default values are Port 1 = 4000, Port 2 = 4001, Port 3 = 4002, Port 4 = 4003.

*Note: On Windows XP SP2 or Windows Server 2003, the installation process configures the Windows firewall for Telnet Manager. If you are using a third-party firewall, you must manually open these ports or provide an exception for the Telnet Manager service.*

### Terminal ID Mode

#### **MAC Address (SNMP)**

If this option is selected, IBM 5250 Telnet Manager uses the MAC address to identify the mobile device. If an SNMP agent is in use, this option should be enabled.

#### **IP Address (Legacy)**

If this option is selected, IBM 5250 Telnet Manager uses the IP address to identify the mobile device. If using legacy (DOS) devices, this option should be enabled.

### Radio Server Fast Failover

Radio server fast failover is not supported on the IBM 5250 Telnet Manager.

### TCP/IP Host KeepAlive

The TCP/IP Host KeepAlive function prevents the TCP/IP socket connection between the application host and Telnet Manager from being torn down if the host is present. In a situation where there is no traffic between the host and Telnet Manager for a long time, Telnet Manager sends a KeepAlive message to the host computer. If the host responds, Telnet Manager knows the host is still present and keeps the socket open. If the host does not respond to repeated Keep-

---

Alive messages, Telnet Manager closes the socket to the host. This disables communications between the host and Telnet Manager until a new socket is negotiated. If Telnet Manager closes the host socket, it also closes the socket opened to the client computer as well. (With no host, there is no point in keeping the client connected.)

The Host KeepAlive function plays a role only if there has been no activity on the Telnet Manager / host link for a period of time. The Host KeepAlive timer is reset on every message received from the host computer. The Host KeepAlive function is useful to detect a failure on the host communications link during periods of inactivity. If the host connection is lost and Telnet Manager closes the socket, it also issues a Host KeepAlive SNMP Trap message.

Telnet session 'keep-alive' is controlled by three parameters:

**Initial delay in milliseconds:** This is the length of time of no activity from the host before sending the KeepAlive message.

**Retry Interval in milliseconds:** The length of time between KeepAlive message retries.

**Disable Host KeepAlive:** This parameter enables or disables the telnet session 'keep-alive' functionality.

### ***Disable***

This checkbox governs the host KeepAlive behavior of the IBM 5250 Telnet Manager.

If the Host KeepAlive function is disabled, Telnet Manager does not send KeepAlive messages to the host computer, and does not close the socket to the host during periods of inactivity on the link.

When checked, the host KeepAlive is disabled. When checked, this control causes other data entry fields in this section to be disabled.

### ***Initial delay in milliseconds***

This text field indicates the duration of inactivity on the host link that Telnet Manager waits before sending a KeepAlive message to the host. The value is specified in milliseconds, and is validated for an integer number in the range 300,000 – 7,200,000.

Default value for this field is 7200000 milliseconds (2 hours).

### ***Retry interval in milliseconds***

This text field indicates the time to wait before sending another Host KeepAlive message if the host has not responded to the previous KeepAlive message(s). The host socket is closed, and a Host KeepAlive SNMP trap is issued, if the host does not respond to 5 consecutive KeepAlive messages. The value of the "Retry interval in milliseconds" field is specified in milliseconds, and is validated for an integer number in the range 10,000 – 75,000.

Default value for this field is 75000 milliseconds (1.25 minutes).

### ***Connection Response Delay***

Provides a delay between when the computer connects to the Telnet Manager and when Telnet Manager issues the request for the LU# from the computer.

The value of the "Connection response delay" field is specified in milliseconds, and is validated for an integer number in the range 1 – 2,000.

Default value for this field is 250 milliseconds.

### ***SNMP Traps***

SNMP Traps are logged for the following actions:

Application host communications failure. An alarm event Trap is generated if Telnet Manager loses communications with any host for which a session is currently open.

Terminal communications failure. Telnet Manager generates an alarm event if a specific client device is disconnected due to a 'keep-alive' time out more than a specified number of times.

Telnet Manager Boot. When Telnet Manager goes through a Boot for whatever reason a "Boot Trap" is sent.

### ***Enable***

This checkbox controls the Telnet Manager SNMP Trap function.

---

When checked, Telnet Manager sends traps to the Trap Destination IP address (see below). When deselected, Telnet Manager does not send SNMP traps. When deselected, this control causes other data entry fields in this section to be disabled.

The default value for this checkbox is deselected.

### **Community Name**

This text field indicates the SNMP community name. This field is validated for a string with a maximum length of 32 characters.

Default value for this field is 'public'.

### **Host**

This text field indicates the IP address or Domain Name of the network manager that is to receive SNMP trap messages generated by the IBM 5250 Telnet Manager. This field is NOT validated for correct IP address format (1.0.0.0 to 254.254.254.254).

Default value for this field is 10.0.0.1.

### **Port**

This text field indicates the IP port number on the network manager station to receive SNMP trap messages. This field is validated for a legal port number (an integer in the range 1 – 65535).

Default value for this field is 162.

## **Log File**

### **Disable**

When checked, no log file is kept.

The default is unchecked – a log file is maintained by Telnet Manager.

### **Limit Maximum Size**

This option determines the maximum file size (in MB) that Telnet Manager maintains for the log file. Once the maximum size is reached, Telnet Manager starts a new log file.

The default is unchecked – no limit on log file size.

To enable, check the box and specify a maximum file size in MB in the text box.

### **Limit Maximum Number**

This option determines the maximum number of log files that can accumulate before deleting the oldest log file. A new log file is created when either of the following occurs:

- The maximum file size is reached (see the parameter above)
- The Telnet Manager service is restarted.

The default is unchecked – no limit on the number of log files maintained.

To enable, check the box and specify the number of log files to keep.

### **Directory**

This text parameter holds the name of the directory path for the IBM 5250 Telnet Manager log file.

Default value for this field is <install directory>\5250\LOG (when installed in the default directory, C:\Program Files\Honeywell\Telnet Manager\5250\log or C:\Program Files (x86)\Honeywell\Telnet Manager\5250\log).

This text parameter holds the name of the directory path for the ANSI Telnet Manager log file.

This field is validated to ensure the directory already exists.

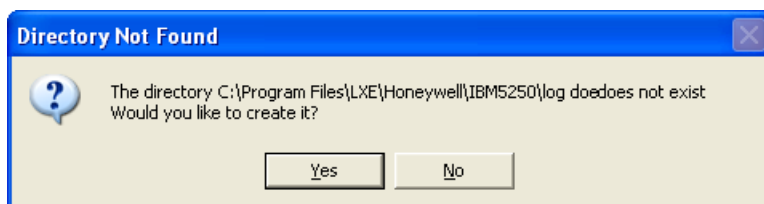
The Browse button can be used to select a location for the log file.

---

## Dialog / Error Boxes

### Directory Does Not Exist

If the debug log file directory does not exist when the 'Save Current Values' button is clicked, a dialog box alerts the user and asks if the directory is to be created.



#### Select Yes

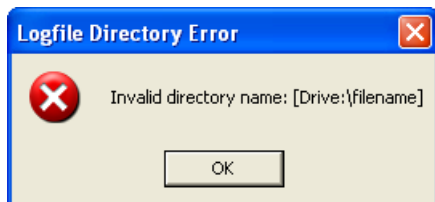
The directory specified in the Debug Log File Directory location is created and the dialog box is removed from the display.

#### Select No

The directory specified in the Debug Log File Directory location control is not changed from the previously saved value. The dialog box is removed from the display.

### Logfile Directory Error

If the debug log file directory specified when the 'Save All Current Values' button is selected is not formatted as a valid directory string, a dialog box reminds the user of the format for a valid directory path.



#### Select OK

The directory specified in the Debug Log File Directory location control is not changed from the previously saved value. The dialog box is removed from the display.

#### Select Close control

Equivalent to the OK button.

### Parameter Change Notification

When the new Global Configuration parameters have been saved, a dialog box appears that states the new parameters do not take effect until Telnet Manager is restarted.



#### Select OK

The dialog box is removed from the display.



---

### **Select Close control**

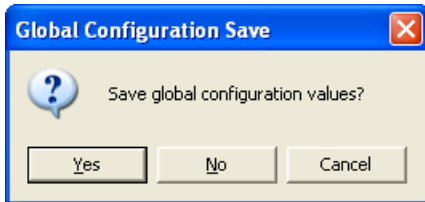
Equivalent to the OK button.

After dismissing the notification, to restart TM1Service, click the Restart Service button on the Global Configuration screen. For more information on Tm1Service, including alternative methods of restarting the service, see [TM1 Service](#) (page 29).

*Note: Restarting the service terminates any existing client connections.*

### **Global Configuration Save**

If the Global Configuration item in the browser tree loses focus (some other item in the browser tree is selected or the IBM 5250 TM1Config interface is closed), the panel is checked for unsaved changes. If any unsaved changes are detected, a dialog box is displayed to notify the user and request the desired action.



#### **Select Yes**

All user modifiable fields displayed in this panel are saved for use by the IBM 5250 Telnet Manager. These are the values that are displayed the next time the Global Configuration item in the browser tree is selected. The dialog box is removed from the display.

#### **Select No**

The current session's user modified values in this panel are discarded and no changes are made. The previously saved values are displayed the next time the Global Configuration item in the browser tree is selected. The dialog box is removed from the display.

#### **Select Cancel**

Focus is restored to the Global Configuration item in the browser panel and no changes are made.

None of the field values are altered and the dialog box is removed from the display.

#### **Select Close control**

Equivalent to the Cancel button.

## **IBM 5250 Client Registration**

Selecting the Client Registration item in the browser panel causes no action other than to highlight the Client Registration text and icon in the browser panel.

Selecting this choice causes the "Register a Terminal" interface to be displayed in the Register a terminal panel to appear.

## Registering New Client Devices

The screenshot shows a window titled "TM1 IBM5250 Configuration Utility" with a sidebar containing "Global Configuration" and "Client Registration". The main area is titled "Register a terminal" and contains two input fields: "Terminal identification:" with a text box, and "Terminal incoming connection port:" with a dropdown menu showing "4000". Below these fields is an "Add New" button.

### Factory Defaults

Terminal Identification	Blank
Terminal incoming connection port	Value assigned to Port 1 in the Global Configuration panel.

### Buttons

#### Add New

Clicking this button causes the specified client identification string and port number to be added to the IBM 5250 Telnet Manager database and the browser panel display is refreshed to include the newly defined client device.

Newly registered client devices are assigned configuration parameters from the Client Registration Master Template in effect at the time the device is registered. If the Terminal Identification field is blank, there is no action.

### Parameters

#### Terminal Identification

This text field stores the text string used to identify the new client device.

This field is validated to conform to a format consistent with the Terminal ID Mode selection on the Global Configuration screen.

- If MAC Address (SNMP) is selected, this field must be a text string formatted as a MAC address. MAC address format is six hexadecimal numbers in the range 0 through ff. Colon characters must separate the six numbers. They may be padded with leading zeros, but that is not required. MAC addresses are NOT case sensitive.

- If IP Address (Legacy) is selected, this field must be to conform to IP address formatting standards. The octets of the IP address must NOT be padded with leading zeros.

The default value of this field is blank.

### **Terminal Incoming Connection Port**

Select a port from the drop down list. Input is restricted to selecting from the pull-down list. If the value you need does not exist in the pull-down list, it must be added using the Global Configuration panel.

The default value of this field is the value assigned to Port 1 in the Global Configuration panel.

## **Client Registration / Master Template**

Selecting the 'Master Template' item in the browser panel list that is subordinate to Client Registration displays the Terminal Master Template interface in the configuration panel.

Using the mouse right-click function on the 'Master Template' item in the browser panel causes no action.

The screenshot shows the 'TM1 IBM5250 Configuration Utility' window. On the left is a tree view with 'Global Configuration', 'Client Registration', and 'Master Template' (selected). The main area is titled 'Master Template' and contains the following configuration sections:

- Host Connection**
  - Name:  Port:
  - Connection timeout (seconds):
  - Connection Management:
- Ssh**
  - Off
  - Shell
  - Tunnel
  - Select Profile:
  -
- Activity Timeout**
  - Enable
  - Timeout (minutes):
- TCP/IP Terminal KeepAlive**
  - Disable
  - Initial delay (ms):
  - Retry interval (ms):

At the bottom of the panel are two buttons: 'Restore factory default values' and 'Save current values'.

---

## Factory Defaults

Host Connection	Name: 10.0.0.1 Port: 23 Connection timeout in seconds: 10 seconds Connection Management: Always maintain connection
SSH	Off: Selected (SSH is disabled) Shell: Not Available Tunnel: Unselected Select Profile : N/A
Activity Timeout	Enable: Disabled Timeout (minutes): 5
TCP/IP Terminal KeepAlive	Disable: Enable Initial delay (ms): 7200000 milliseconds (2 hours) Retry interval (ms): 75000 milliseconds (1.25 minutes)

## Buttons

### **Edit/Create Profile**

This button is active only if SSH Tunnel or SSH Shell is selected. When active, this button accesses the [SSH Settings](#) (page 109) screen.

### **Restore Values to Factory Default**

Clicking this button causes all user modifiable fields to be restored to the factory default values.

### **Save current values**

Clicking this button causes all user modifiable fields displayed in this panel to be saved for use by the IBM 5250 Telnet Manager.

These are the values that are displayed the next time the Client Registration / Master Template item in the browser tree is selected.

Values in the Master Template are automatically propagated to the registered terminals. All configuration items for all registered terminals that have not been changed from the Master Template values are immediately updated to reflect the new Master Template configuration.

*Note: Configuration values for registered terminals that have been changed from the Master Template value are not affected.*

## Parameters

In some cases, system administrators are concerned about having client devices logged in but inactive. In these cases, Telnet Manager provides the ability to log the client device off the host if there has been no user activity for a specified time period. The parameters used to manage RF client devices are Host Connection, Manage Terminal Session, and Activity Timeout.

### **Host Connection**

#### **Name**

Enter the IP address or Domain Name of the host computer to which this client device connects into this text field. This field is validated for correct IP address format (1.0.0.0 to 254.254.254.254).

The default value of this field is 10.0.0.1.

*Note: If Use SSH Tunnel (see below) is selected this field is set to 127.0.0.1 and cannot be edited as long as the SSH option is enabled.*

---

## **Port**

This text field indicates the IP port number on the application host to which this client connects. This field is validated for a legal port number (an integer number in the range 1 – 65535).

Default value for this field is 23.

*Note: If Use SSH Tunnel (see below) is selected, the value in this field must be set to the listening port specified in the SSH profile.*

## **Connection Timeout (seconds)**

Enter the host connection timeout value in this text field. This field is validated for an integer in the range 5 – 65535.

Default value for this field is 10.

## **Connection Management**

Use this option to determine the type of Host Connection Management:

- Always close connection
- Always maintain connection (default)
- Close connection on explicit close.

## **SSH**

### **Off**

Telnet is used without SSH.

### **Shell**

This option is not available for IBM 5250.

### **Tunnel**

A connection is established to an SSH server and Telnet traffic is tunneled (port forwarded) through the SSH connection.

*Note: This checkbox can only be accessed if the Include SSH option was selected during installation. Uninstall Telnet Manager and reinstall with the Include SSH option selected to enable this feature.*

## **Select Profile**

Select the name of a previously created SSH connection profile to use. If no profiles exist or to modify an existing profile, use the **Edit/Create Profile** button to access the [SSH Settings](#) (page 109) screen to create or modify a profile.

## **Activity Timeout**

The Activity Timeout allows the administrator to logoff a client computer that has been idle for a specified period of time. The client computer is logged off, and a Session Disconnect Activity timeout SNMP Trap is issued, regardless of whether or not the client computer is present on the network. Telnet Manager closes both the socket to the client computer and to the host computer. If this client computer subsequently reconnects to Telnet Manager, it is assigned to a new host session.

### **Enable**

Selecting this checkbox enables the activity timeout feature for this client device. If this checkbox is cleared, data entry in the Timeout in Minutes field is disabled.

The default state of this checkbox is not selected.

### **Timeout (minutes)**

This text field is used to enter the activity timeout value for this client device. This field is validated for an integer in the range 5 – 65535.

If the Enable checkbox is not selected, data entry in this field is disabled.

Default value for this field is 5.

---

## **TCP/IP Terminal KeepAlive**

The TCP/IP Terminal KeepAlive function prevents the TCP/IP socket connection between the individual client computer and Telnet Manager from being torn down if the client computer is present. In a situation where there is no traffic between the client computer and Telnet Manager for a long time, Telnet Manager sends a KeepAlive message to the client. If the client responds, Telnet Manager knows the client is still present and keeps the socket open. If the client computer does not respond to repeated KeepAlive messages, Telnet Manager closes the socket to the client computer. This disables communications between this particular client computer and Telnet Manager until a new socket is negotiated.

The Terminal KeepAlive function plays a role only if there has been no activity on the Telnet Manager / client computer link for a period of time. The Terminal KeepAlive timer is reset on every message received from the client computer. The Terminal KeepAlive function is useful to close unused client computer sockets. If the client computer connection is lost and Telnet Manager closes the socket, it also issues a TE Disconnect SNMP Trap message.

Note that if Telnet Manager closes the client computer socket because the client does not respond to TCP/IP KeepAlive messages, it does not close the corresponding socket to the host computer. If the same client computer reconnects later, it is reconnected to the same host socket – that is, it is reconnected to the same session it had before.

### **Disable**

This control governs the terminal KeepAlive behavior of the IBM 5250 Telnet Manager.

When selected, terminal KeepAlive is disabled and causes the other data entry fields in this section to be disabled. If the Terminal KeepAlive function is disabled, Telnet Manager does not send KeepAlive messages to the client computer, and does not close the socket to the client during periods of inactivity on the link.

When cleared, terminal KeepAlive is enabled.

The default value for this checkbox is cleared.

### **Initial delay (ms)**

This text field indicates the duration of inactivity on the client computer link that Telnet Manager waits before sending a KeepAlive message to the client. The value is specified in milliseconds, and is validated for an integer number in the range 300,000 – 7,200,000.

Default value for this field is 7200000 milliseconds (2 hours).

### **Retry interval (ms)**

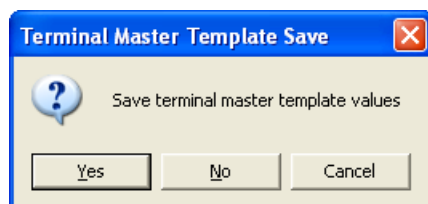
This text field indicates the time to wait before sending another Terminal KeepAlive message if the client computer has not responded to the previous KeepAlive message(s). The client socket is closed, and a TE Disconnect SNMP trap is issued, if the client does not respond to 5 consecutive KeepAlive messages. The value of the “Retry interval in milliseconds” field is specified in milliseconds, and is validated for an integer number in the range 10,000 – 75,000.

Default value for this field is 75000 milliseconds (1.25 minutes).

## **Dialog / Error Boxes**

### **Terminal Master Template Save**

If the Client Registration Master Template item in the browser tree loses focus (some other item in the browser tree is selected or the IBM 5250 TM1Config interface is closed), the panel is checked for unsaved changes. If any unsaved changes are detected, a dialog box is displayed to notify the user and request the desired action.



---

### **Select Yes**

All user modifiable fields displayed in this panel are saved for use by the IBM 5250 Telnet Manager. These are the values that are displayed the next time the Client Registration Master Template item in the browser tree is selected. The dialog box is removed from the display.

### **Select No**

The current session's user modified values in this panel are discarded and no changes are made. The previously saved values are displayed the next time the Client Registration Master Template item in the browser tree is selected. The dialog box is removed from the display.

### **Select Cancel**

Focus is restored to the Client Registration Master Template item in the browser panel and no changes are made.

None of the field values are altered and the dialog box is removed from the display.

### **Select Close control**

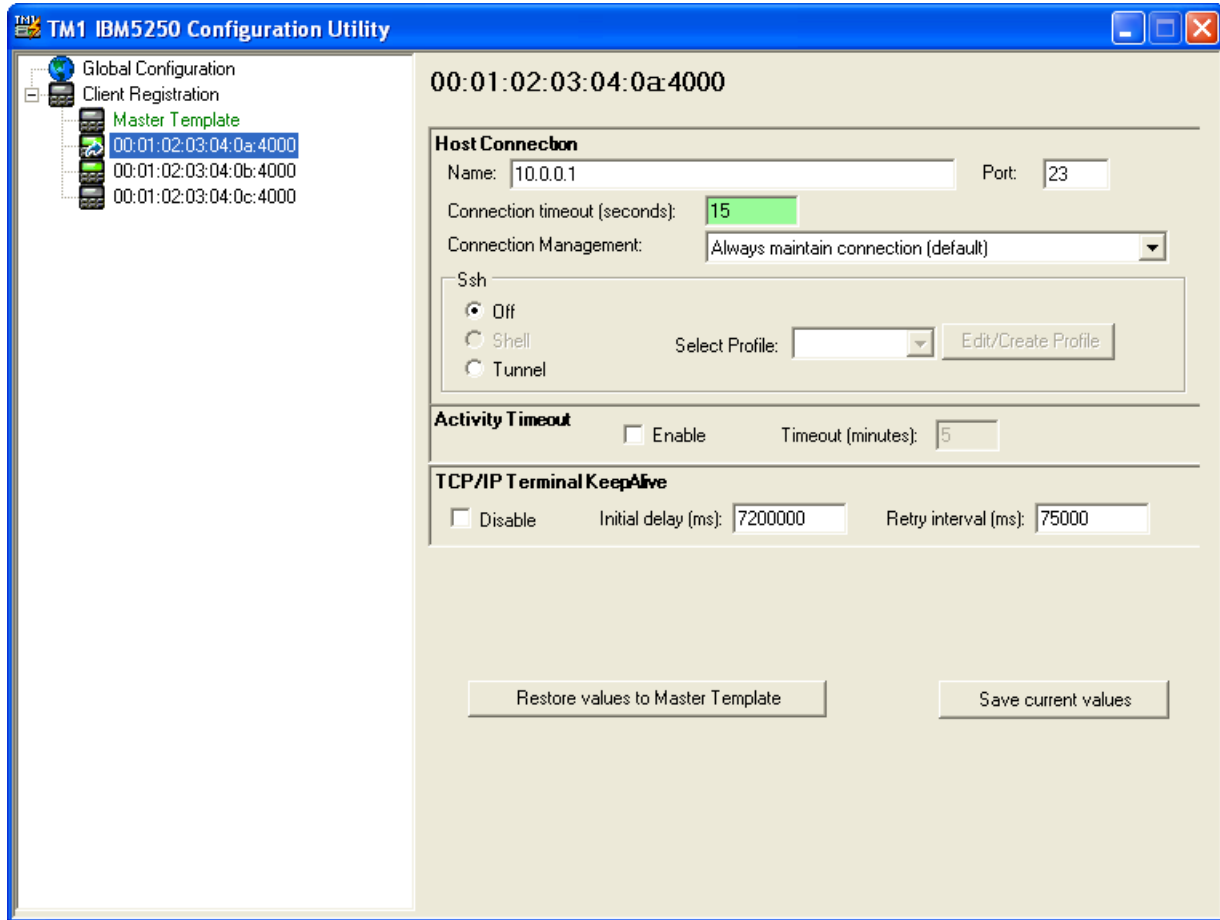
Equivalent to the Cancel button.

## **Client Registration / Registered Clients**

Selecting any of the individual client ID items in the browser panel list that is subordinate to Client Registration displays the Registered Terminal interface in the configuration panel.

If any of the configurable parameters in this configuration panel display differ from the corresponding parameters in the Master Template configuration panel, those controls are highlighted. Likewise the Registered Client icon is also highlighted for any clients whose saved values differ from the Master Template values.

A right mouse click on the selected individual client ID item, displays a one-line menu item – to delete the highlight registered client. Refer to [Removing a Registered Client](#) (page 105) for instruction.



### Factory Defaults

Host Connection	Name: Host Connection IP address of the host computer from the Master Template. Port: Host Connection Port value from the Master Template. Connection timeout in seconds: Host Connection Timeout value From the Master Template. Connection Management: Value from the Master Template.
SSH	Off, Tunnel: Value from the Master Template Select Profile: Value from the Master Template
Activity Timeout	Enable: Activity Timeout Enable checkbox from the Master Template. Timeout (minutes): Activity Timeout / Timeout in Minutes value from the Master Template.
TCP/IP Terminal KeepAlive	Disable: Disable checkbox status from the Master Template. Initial delay (ms): TCP/IP Terminal KeepAlive / Initial delay in milliseconds value from the Master Template. Retry interval (ms): TCP/IP Terminal KeepAlive / Retry interval in milliseconds value from the Master Template.

### Buttons

#### **Edit/Create Profile**

This button is active only if SSH Tunnel or SSH Shell is selected. When active, this button accesses the [SSH Settings](#) (page 109) screen.



---

### **Restore Values to Master Template**

Clicking this button causes all user modifiable fields to be restored to the values defined by the current Client Configuration Master Template.

### **Save current values**

Clicking this button causes all user modifiable fields displayed in this panel to be saved for use by the IBM 5250 Telnet Manager.

These are the values that are displayed the next time this Client ID is selected in the Client Registration branch of the browser tree.

### **Parameters**

In some cases, system administrators are concerned about having client devices logged in but inactive. In these cases, Telnet Manager provides the ability to log the client device off the host if there has been no user activity for a specified time period. The parameters used to manage RF client devices are Host Connection, Manage Terminal Sessions, and Activity Timeout.

#### **Host Connection**

##### **Name**

Enter the IP address or Domain Name of the host computer to which this client device connects into this text field. This field is validated for correct IP address format (1.0.0.0 to 254.254.254.254).

The default value of this field is the Host Connection IP Address value from the Master Template.

##### **Port**

This text field indicates the IP port number on the application host to which this client connects. This field is validated for a legal port number (an integer number in the range 1 – 65535).

Default value for this field is the Host Connection Port value from the Master Template.

*Note: If Use SSH Tunnel (see below) is selected, the value in this field must be set to the listening port specified in the SSH profile.*

##### **Connection Timeout (seconds)**

Enter the host connection timeout value in this text field. This field is validated for an integer in the range 5 – 65535.

Default value for this field is the Host Connection Timeout in Seconds value from the Master Template.

##### **Connection Management**

Use this option to determine the type of Connection Management:

- Always close connection
- Always maintain connection (default)
- Close connection on explicit close.

##### **SSH**

Default value for SSH is the connection type from the Master Template.

##### **Off**

Telnet is used without SSH.

##### **Shell**

This option is not available for IBM 5250.

##### **Tunnel**

A connection is established to an SSH server and Telnet traffic is tunneled (port forwarded) through the

---

SSH connection.

*Note: If this option is enabled on the Client Registration Master Template, the default SSH tunnel is created at TM1 startup. If a different SSH tunnel connection profile is used for a registered terminal, there may be a delay when first connecting as it can take up to 20 seconds to establish an SSH tunnel.*

### **Select Profile**

Select the name of a previously created SSH connection profile to use. If no profiles exist or to modify an existing profile, use the **Edit/Create Profile** button to access the [SSH Settings](#) (page 109) screen.

The default value is the profile (if any) from the Master Template.

### **Activity Timeout**

The Activity Timeout allows the administrator to logoff a client computer that has been idle for a specified period of time. The client computer is logged off, and a Session Disconnect Activity timeout SNMP Trap is issued, regardless of whether or not the client computer is present on the network. Telnet Manager closes both the socket to the client computer and to the host computer. If this client computer subsequently reconnects to Telnet Manager, it is assigned to a new host session.

#### **Enable**

Selecting this checkbox enables the activity timeout feature for this client device. If this checkbox is cleared, data entry in the Timeout in Minutes field is disabled.

Default state for this checkbox is the state of the Activity Timeout Disable checkbox from the Master Template.

#### **Timeout (minutes)**

This text field is used to enter the activity timeout value for this client device. This field is validated for an integer in the range 5 – 65535.

Default value for this field is the Activity Timeout / Timeout in Minutes value from the Master Template.

### **TCP/IP Terminal KeepAlive**

The TCP/IP Terminal KeepAlive function prevents the TCP/IP socket connection between the individual client computer and Telnet Manager from being torn down if the client computer is present. In a situation where there is no traffic between the client computer and Telnet Manager for a long time, Telnet Manager sends a KeepAlive message to the client. If the client responds, Telnet Manager knows the client is still present and keeps the socket open. If the client computer does not respond to repeated KeepAlive messages, Telnet Manager closes the socket to the client computer. This disables communications between this particular client computer and Telnet Manager until a new socket is negotiated.

The Terminal KeepAlive function plays a role only if there has been no activity on the Telnet Manager / client computer link for a period of time. The Terminal KeepAlive timer is reset on every message received from the client computer. The Terminal KeepAlive function is useful to close unused client computer sockets. If the client computer connection is lost and Telnet Manager closes the socket, it also issues a TE Disconnect SNMP Trap message.

Note that if Telnet Manager closes the client computer socket because the client does not respond to TCP/IP KeepAlive messages, it does not close the corresponding socket to the host computer. If the same client computer reconnects later, it is reconnected to the same host socket – that is, it is reconnected to the same session it had before.

#### **Disable**

This control governs the terminal KeepAlive behavior of the IBM 5250 Telnet Manager.

When selected, terminal KeepAlive is disabled and causes the other data entry fields in this section to be disabled. If the Terminal KeepAlive function is disabled, Telnet Manager does not send KeepAlive messages to the client computer, and does not close the socket to the client during periods of inactivity on the link.

When cleared, terminal KeepAlive is enabled.

The default value for this field is the Disable checkbox status from the Master Template.

---

### **Initial delay (ms)**

This text field indicates the duration of inactivity on the client computer link that Telnet Manager waits before sending a KeepAlive message to the client. The value is specified in milliseconds, and is validated for an integer number in the range 300,000 – 7,200,000.

Default value for this field is the TCP/IP Terminal KeepAlive / Initial delay in milliseconds value from the Master Template or 7200000 milliseconds (2 hours).

### **Retry interval (ms)**

This text field indicates the time to wait before sending another Terminal KeepAlive message if the client computer has not responded to the previous KeepAlive message(s). The client socket is closed, and a TE Disconnect SNMP trap is issued, if the client does not respond to five consecutive KeepAlive messages.

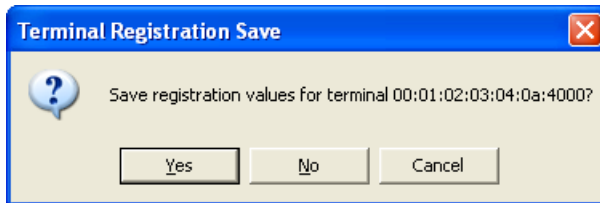
The value of this field is specified in milliseconds, and is validated for an integer number in the range 10,000 – 75,000.

Default value for this field is the TCP/IP Terminal KeepAlive / Retry interval in milliseconds value from the Master Template.

## **Dialog / Error Boxes**

### **Terminal Registration Save**

If the Client Registration individual client ID item in the browser tree loses focus (some other item in the browser tree is selected or the IBM 5250 TM1Config interface is closed), the panel is checked for unsaved changes. If any unsaved changes are detected, a dialog box is displayed to notify the user and request the desired action.



#### **Select Yes**

All user modifiable fields displayed in this panel are saved for use by the IBM 5250 Telnet Manager. These are the values that are displayed the next time this individual client ID item in the browser tree is selected. The dialog box is removed from the display.

#### **Select No**

The current session's user modified values in this panel are discarded and no changes are made. The previously saved values are displayed the next time this individual client ID is selected. The dialog box is removed from the display.

#### **Select Cancel**

Focus is restored to the Client Registration Master Template in the browser panel and no changes are made. None of the field values are altered and the dialog box is removed from the display.

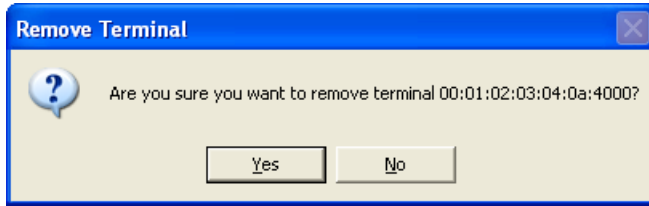
#### **Select Close control**

Equivalent to the Cancel button.

### **Removing a Registered Client**

Using the mouse right-click function in the browser panel when one of the individual client ID items has focus (is highlighted) causes an option menu to be displayed.

The option menu contains the single choice to remove the selected client. Selecting this choice causes the "Remove Terminal" dialog box to be displayed. The dialog box requests the user for confirmation to remove the selected terminal registration. The individual client ID text and icon retain their highlighted (selected) status until the removal is confirmed.



### **Select Yes**

Selecting this option causes the specified terminal registration to be removed and entries for this terminal are removed and are no longer available to the IBM 5250 Telnet Manager. The browser panel is refreshed to show the browser tree without the removed terminal. Focus in the browser panel shifts to the terminal that previously followed the removed terminal.

If the removed terminal was the last terminal in the list, focus shifts to the preceding terminal in the list. If the removed terminal was the only terminal in the list, focus shifts to the Client Registration Master Template

The configuration panel is refreshed to reflect the item now selected in the browser panel and the Remove Terminal dialog box is removed from the display.

### **Select No**

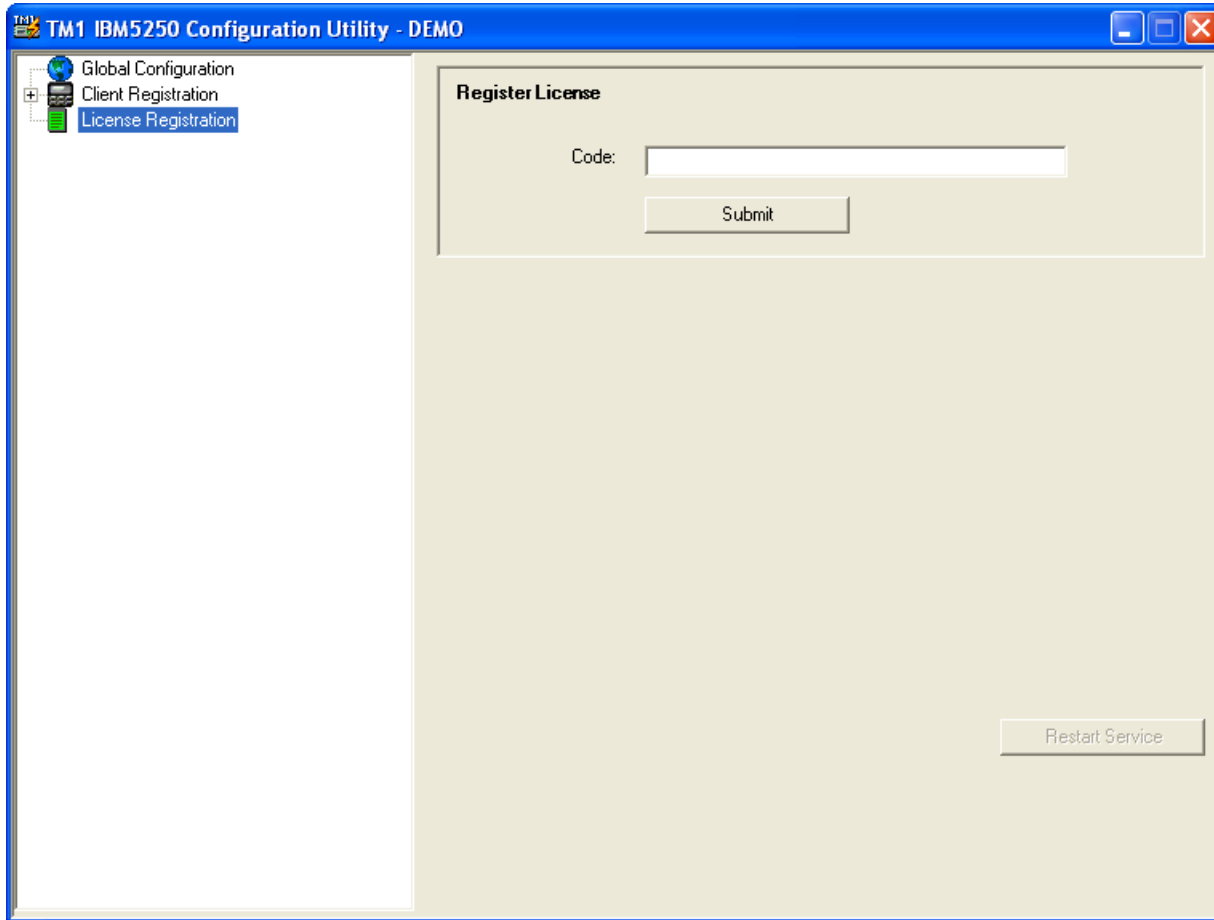
The specified terminal registration is retained and the Remove Terminal dialog box is removed from the display.

## **License Registration**



The License Registration option is only displayed in the Browser Panel if a valid license key has not previously been entered.

Telnet Manager remains in Demo mode until a valid license key is entered. To enter a license key, click on the License Registration branch.



If Telnet Manager was purchased, a license key was included. Refer to the License Key letter provided for the key. Note that the key is case sensitive.

Contact [Technical Assistance](#) (page 1) with any purchase or license key questions.

When the key is entered, click the submit button to verify the key.

## **Buttons**

### **Submit**

The submit button verifies the license key entered.

If a valid license key is entered, a “success” message is displayed. Telnet Manager is no longer in demo mode.

The DEMO notation in the title bar, the “days remaining” message and the License Registration branch are all removed when TM1Config is next initiated.

If an error message is displayed, double check the key. Remember, the license key is case sensitive. Telnet Manager remains in Demo mode until a valid key is entered.

### **Restart Service**

Clicking this button stops and restarts the TM1 service. If the service is not already running, this button starts the service. This button is not active on this screen until a valid license key is entered.

*Note: Restarting the service terminates any existing client connections.*



## SSH Settings

### Introduction

The SSH settings screen can be accessed from either the Master Template or a Registered Client by clicking the **Edit/Create Profile** button.

*Note: Profiles are global. A profile created under one client can be accessed by any other clients.*

### Select Profile

#### Select Profile List

If the **Select Profile** radio button is selected, the pull down list allows a previously saved profile to be selected. Once a profile is selected, the screen is populated with the values from that profile.

#### Create New Profile

If the **Create New Profile** radio button is selected, the text box for Profile Name is available to enter a name for the new profile.

#### Profile Name

Use the text box to enter a name for the new profile.

---

## **Save Profile**

Click the **Save Profile** button to either:

- Save the current settings as the new values for the selected profile if **Select Profile** is active.
- Save the current settings as a new profile with the name specified in the **Profile Name** textbox if **Create New Profile** is active.

## **SSH Server**

### **Address**

Enter the IP address of the SSH server.

### **Port**

Enter the port for the SSH server.

## **Authorization**

Select the type of authorization, either User Name and Password or Key file.

### **User+Pswd**

When selected, enter the appropriate credentials for authentication.

#### **User**

Enter the user name for SSH authentication.

#### **Password**

Enter the password for SSH authentication.

### **Key File**

Private key file authentication requires a user name, a private key file and an optional passphrase for the key file. Use the [PuTTY Key Generator](#) (page 111) to create a private key file.

#### **User**

Enter the user name for SSH authentication.

#### **Passphrase**

An optional passphrase may be required to use the private key. If a passphrase was specified when the key file was created, the passphrase must be entered.

#### **User Key File**

Only one private key file is stored per session. Use the **Browse...** and **OK** buttons to locate and select the private key file.

Use the PuTTY Key Generator to generate the private key file.

#### **Browse**

Clicking this button opens an explorer window to locate the key file. By default, only PuTTY private key files are displayed in the explorer window.

#### **OK**

After using the **Browse...** button to locate and select a key file, the file location and name are displayed in the **User Key File** text box.

### **Allow connection to unlisted host**

When selected, only hosts included in the Global Allowed Host Key listing are available for connection.



---

It is necessary to check this box and connect to any desired hosts so they are in the Allowed list. Once all desired hosts are included, then uncheck this item to prevent connection to any other hosts.

## **Advanced Settings**

### **Keep Alive Ping Interval**

Use this option to manage SSH Keep Alive messages. The default is 0 minutes (no SSH Keep Alive messages). Any value greater than 0 (whole numbers only) sends SSH Keep Alive messages after the specified number of minutes.

### **Rekey After MB of Data**

The session key is negotiated at session startup. Because the longer a key is used, the greater the chances the connection may be successfully attacked, an option is provided to force a new key exchange (from the server side) after the specified MB of data is exchanged.

The default is 0 MB, no rekey is enabled after a certain amount of data is transferred. Any value greater than 0 (whole numbers only) forces a rekey after that amount of data has been transferred. No data passes through the SSH connection while the rekeying takes place.

*Note: The client may also enable rekeying, so rekeying may still happen even if this option and the one below are disabled.*

### **Rekey After Minutes**

The session key is negotiated at session startup. Because the longer a key is used, the greater the chances the connection may be successfully attacked, an option is provided to force a new key exchange (from the server side) after the specified number of minutes.

The default is 0 minutes, no rekey is enabled after a certain time period. Any value greater than 0 (whole numbers only) forces a rekey after that length of time. No data passes through the SSH connection while the rekeying takes place.

*Note: The client may also enable rekeying, so rekeying may still happen even if this option and the one above are disabled.*

### **Compression**

When enabled, data compression is used. By default, compression is disabled.

## **Server Keys**

### **Global Allowed Host Keys**

The Host Key list is global, meaning a Host Key accepted for use with any profile is displayed in this box.

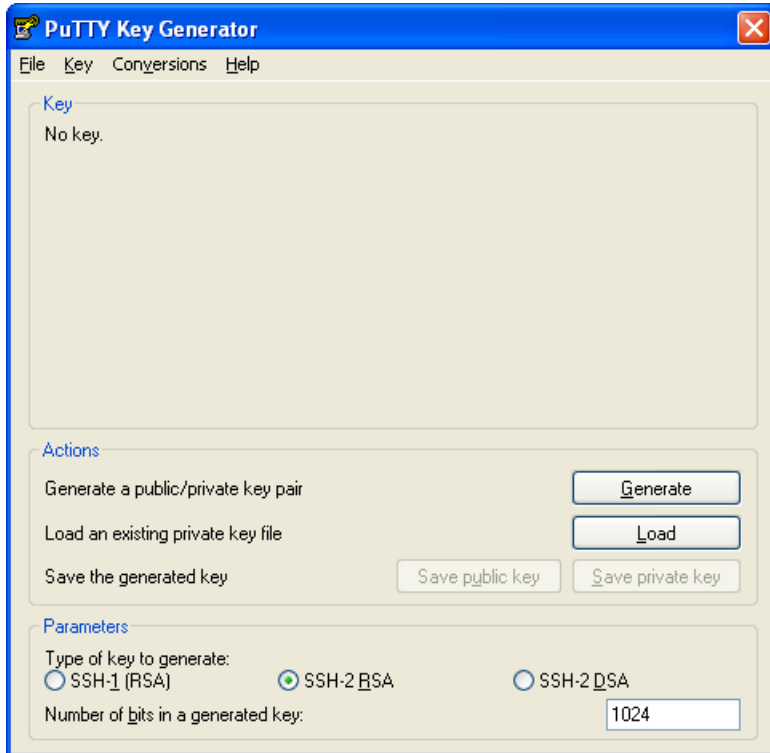
### **Delete**

Select an entry from the Global Allowed Host Key list and tap the **Delete** button to delete a host key entry.

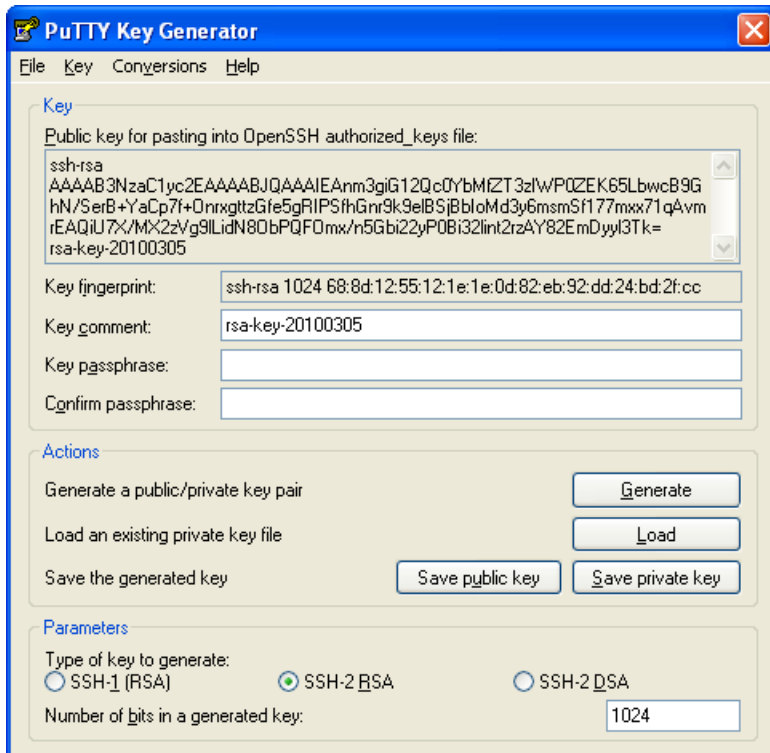
## **PuTTY Key Generator**

Use the PuTTY Key Generator to generate public and private key files.

To access the PuTTY Key Generator, locate and click on the PuttyGen.exe icon in the Telnet Manager installation directory (usually C:\Program Files\Honeywell\Telnet Manager or C:\Program Files (x86)\Honeywell\Telnet Manager).



Click the **Generate** button to generate a key. Follow the on screen prompt to create the key.



---

## ***Public Key***

Click the **Save public key** button to save the public key. Browse to the desired location, enter a file name and click **Save**. This saves a text file containing the public key text for use with the SSH server.

## ***Private Key***

If desired, enter and confirm the Key passphrase. If entered, the passphrase is needed when specifying the private key file in Telnet Manager.

Click the **Save private key** button. Browse to the desired location, enter a file name and click **Save**. This saves a .PPK file (PuTTY Private Key file) in the specified location.

When specifying a private key file browse to the location of this PPK file. When the key file is specified in Telnet Manager the passphrase, if any, must be entered.



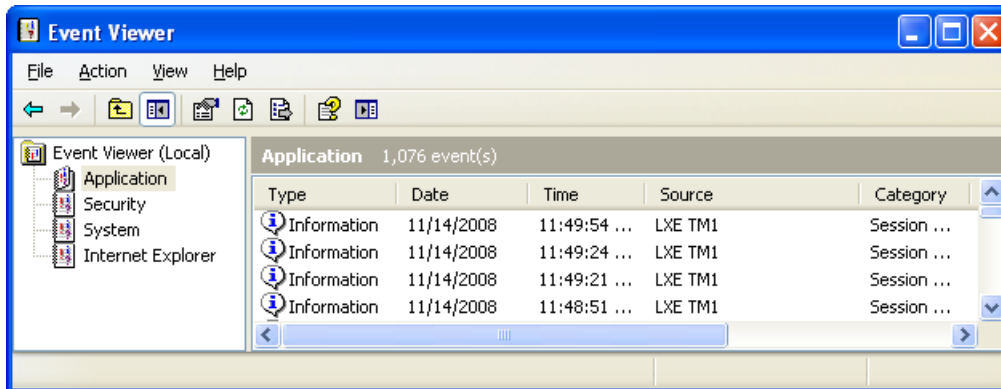
## Logs, SNMP Traps and Reference Material

### Telnet Manager Log Files

#### Windows Event Log

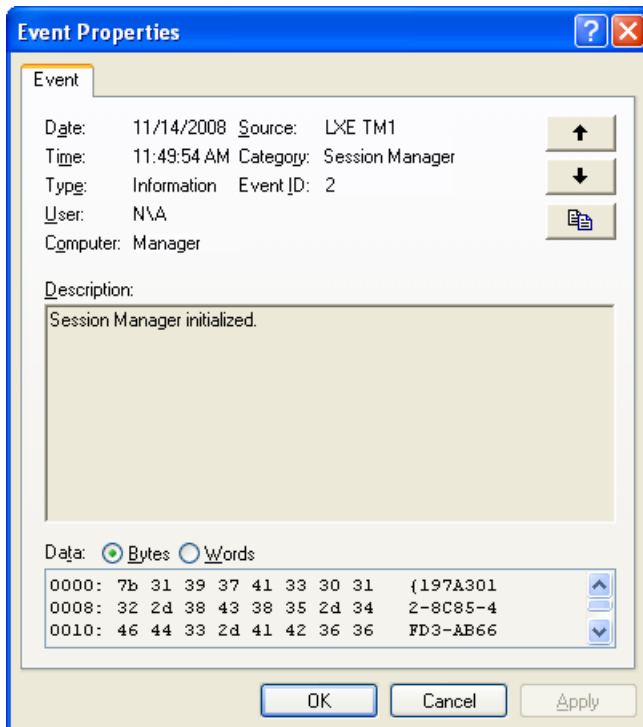
Telnet Manager operation is recorded in the Windows Event log. Access to the Event Viewer may depend on the operating system used:

- Select **Start > Control Panel > Administrative Tools > Event Viewer** and select the Application log.
- Select **Start > Control Panel > Administrative Tools > Event Viewer** and select the Windows Log > Application.



The entries made by Telnet Manager are identified by "Honeywell TM1" in the Source column.

Click on any entry for more details.



For more information on Event Viewer, see the Windows help feature.

---

## Debug Log

The Debug Log level is set using the TM1Console command, sSetDBLevel:

```
sSetDBLevel x
```

Where **x** sets the level of debug information written to the debug log:

x=6: off, only error messages are written (default)

x=5: Least level of detail in debug log file.

x=4: Intermediate level of detail in debug log file.

x=3: Highest level of detail in debug log file.

For more information see [TM1Console](#) (page 31).

The location of the debug log file is specified on the Global Configuration screen of the TM1Config utility. For more information, refer to the appropriate configuration utility for the installed emulation:

- [ANSI Configuration Utility](#) (page 39)
- [IBM 3270 Configuration Utility](#) (page 69)
- [IBM 5250 Configuration Utility](#) (page 89)

*Note: The selected debug log level is in effect only as long as TM1Console remains open. When TM1Console is closed, the debug log level is reset to the default (Off) value and no debug logging is performed.*

### Example Debug Log File

```
Mon Jan 22 13:59:40 2007 Session Manager initialized.  
Mon Jan 22 13:59:40 2007
```

```
TM1 Ready Set Go ...
```

```
Mon Jan 22 13:59:40 2007 CSMListener::issueListen bind port: 4004  
Mon Jan 22 13:59:40 2007 CSMListener::issueListen bind port: 4001  
Mon Jan 22 13:59:40 2007 CSMListener::waitForConnections  
Mon Jan 22 13:59:40 2007 CSMListener::issueListen bind port: 4002  
Mon Jan 22 13:59:40 2007 CSMListener::waitForConnections  
Mon Jan 22 13:59:40 2007 CSMListener::waitForConnections  
Mon Jan 22 13:59:40 2007 CSMListener::issueListen bind port: 4003  
Mon Jan 22 13:59:40 2007 CSMListener::waitForConnections  
Mon Jan 22 14:00:47 2007 Debug level set to 3.
```

---

## SNMP Traps

The SNMP traps generated by Telnet Manager may contain 2 additional variable bindings in addition to the normal trap bindings. The first variable is always "SysUpTime".

The second variable is either the generic trap "ColdStart" or specific "Enterprise" oid. If the trap is of the Enterprise specific type two additional bindings follow.

The third binding is an INT32 type indicating one of the following conditions:

1. Host disconnect socket closed
2. Terminal disconnect socket close
3. Session disconnect autologin failed
4. Session disconnect activity timeout
5. Session disconnect tcp/ip keepalive timeout
6. Terminal unauthorized login reject

The fourth binding is an OCTET STRING which depends on whether the Legacy Mode is enabled or disabled and contains:

- The client device RF MAC address as passed from the device's MIB
- Terminal ID for ANSI Plus
- IP address for IBM 3270 and IBM 5250

<b>ANSI, IBM 3270, IBM 5250 Telnet Manager</b>
Session Disconnect AutoLogin timeout
Session Disconnect Activity timeout
Host KeepAlive
Login Reject
Host Disconnect
TE Disconnect
Cold Start

---

## LXE MIB SNMP Trapping

When installed in the default directory, the MIB is located at:

- C:\Program Files\Honeywell\Telnet Manager (for 32-bit operating systems)
- C:\Program Files (x86)\Honeywell\Telnet Manager (for 64-bit operating systems)

```
LXETM1-MIB DEFINITIONS ::= BEGIN

-- IMPORTS
--   lxeProducts      FROM lxepriv;

IMPORTS
    enterprises
        FROM RFC1155-SMI
    OBJECT-TYPE
        FROM RFC-1212;

DisplayString ::= OCTET STRING
PhysAddress   ::= OCTET STRING

lxe
    OBJECT IDENTIFIER ::= { enterprises 1610 }

lxeRegistration
    OBJECT IDENTIFIER ::= { lxe 1 }
lxeExtensions
    OBJECT IDENTIFIER ::= { lxe 2 }
lxeProducts
    OBJECT IDENTIFIER ::= { lxe 3 }

-- Telnet Manager
lxeProductsTM
    OBJECT IDENTIFIER ::= { lxeProducts 3 }

--Telnet Manager Session Manager Traps
lxeProductsTMSessionManagerTraps
    OBJECT IDENTIFIER ::= { lxeProductsTM 1 }

lxeProductsTMSessionManagerErrorStatus
    OBJECT-TYPE
        SYNTAX INTEGER {autologintimeout(1), activitytimeout(2), tcpkeepalivetimeout(3),
unregisterloginattempt(4), hostdisconnect(5), terminaldisconnect(6)}
        ACCESS read-write
        STATUS mandatory
        DESCRIPTION
            "These values are sent along with the traps."
        ::= { lxeProductsTMSessionManagerTraps 1 }

lxeProductsTMSessionManagerTrap
    NOTIFICATION-TYPE
        OBJECTS { lxeProductsTMSessionManagerErrorStatus, lxeProductsDOSRadioNodeAddress }
        STATUS current
        DESCRIPTION
            "The Telnet Manager issues this trap for certain error conditions."
        ::= { lxeProductsTMSessionManagerTraps 2 }

--Telnet Manager LDSTCP Traps
lxeProductsTMLDSTCPTraps
    OBJECT IDENTIFIER ::= { lxeProductsTM 2 }

lxeProductsTMLDSTCPTermErrorStatus
    OBJECT-TYPE
        SYNTAX INTEGER {terminaltcpkeepalivetimeout(1), hoststackfailed(2)}
        ACCESS read-write
        STATUS mandatory
        DESCRIPTION
            "These values are sent along with the traps."
        ::= { lxeProductsTMLDSTCPTraps 1 }

lxeProductsTMLDSTCPHostErrorStatus
    OBJECT-TYPE
        SYNTAX INTEGER {hosttcpkeepalivetimeout(3), hostdisconnect(4), hostconnectionfailed(5)}
        ACCESS read-write
```



```

STATUS mandatory
DESCRIPTION
"These values are sent along with the traps."
 ::= { lxeProductsTMLDSTCPTraps 2 }

lxeProductsTMLDSTCPTermTrap NOTIFICATION-TYPE
  OBJECTS { lxeProductsTMLDSTCPTermErrorStatus, lxeProductsDOSRadioNodeAddress }
  STATUS current
  DESCRIPTION
"The Telnet Manager issues this trap for certain error conditions."
 ::= { lxeProductsTMLDSTCPTraps 3 }

lxeProductsTMLDSTCPHostTrap NOTIFICATION-TYPE
  OBJECTS { lxeProductsTMLDSTCPHostErrorStatus }
  STATUS current
  DESCRIPTION
"The Telnet Manager issues this trap for certain error conditions."
 ::= { lxeProductsTMLDSTCPTraps 4 }

-- end of lxe Telnet Manager mib definition

END

```

## Decimal – Hexadecimal Equivalents

Note: Hexadecimal numbers in the following chart are assumed to have 6 preceding zeros, i.e., Decimal 20 is Hexadecimal 0000014 and Decimal 220 is Hexadecimal 00000DC.

Dec	Hex	Dec	Hex	Dec	Hex	Dec	Hex	Dec	Hex	Dec	Hex	Dec	Hex	Dec	Hex
0	00	32	20	64	40	96	60	128	80	160	A0	192	C0	224	E0
1	01	33	21	65	41	97	61	129	81	161	A1	193	C1	225	E1
2	02	34	22	66	42	98	62	130	82	162	A2	194	C2	226	E2
3	03	35	23	67	43	99	63	131	83	163	A3	195	C3	227	E3
4	04	36	24	68	44	100	64	132	84	164	A4	196	C4	228	E4
5	05	37	25	69	45	101	65	133	85	165	A5	197	C5	229	E5
6	06	38	26	70	46	102	66	134	86	166	A6	198	C6	230	E6
7	07	39	27	71	47	103	67	135	87	167	A7	199	C7	231	E7
8	08	40	28	72	48	104	68	136	88	168	A8	200	C8	232	E8
9	09	41	29	73	49	105	69	137	89	169	A9	201	C9	233	E9
10	0A	42	2A	74	4A	106	6A	138	8A	170	AA	202	CA	234	EA
11	0B	43	2B	75	4B	107	6B	139	8B	171	AB	203	CB	235	EB
12	0C	44	2C	76	4C	108	6C	140	8C	172	AC	204	CC	236	EC
13	0D	45	2D	77	4D	109	6D	141	8D	173	AD	205	CD	237	ED
14	0E	46	2E	78	4E	110	6E	142	8E	174	AE	206	CE	238	EE
15	0F	47	2F	79	4F	111	6F	143	8F	175	AF	207	CF	239	EF
16	10	48	30	80	50	112	70	144	90	176	B0	208	D0	240	F0
17	11	49	31	81	51	113	71	145	91	177	B1	209	D1	241	F1
18	12	50	32	82	52	114	72	146	92	178	B2	210	D2	242	F2

Dec	Hex	Dec	Hex	Dec	Hex	Dec	Hex	Dec	Hex	Dec	Hex	Dec	Hex	Dec	Hex
19	13	51	33	83	53	115	73	147	93	179	B3	211	D3	243	F3
20	14	52	34	84	54	116	74	148	94	180	B4	212	D4	244	F4
21	15	53	35	85	55	117	75	149	95	181	B5	213	D5	245	F5
22	16	54	36	86	56	118	76	150	96	182	B6	214	D6	246	F6
23	17	55	37	87	57	119	77	151	97	183	B7	215	D7	247	F7
24	18	56	38	88	58	120	78	152	98	184	B8	216	D8	248	F8
25	19	57	39	89	59	121	79	153	99	185	B9	217	D9	249	F9
26	1A	58	3A	90	5A	122	7A	154	9A	186	BA	218	DA	250	FA
27	1B	59	3B	91	5B	123	7B	155	9B	187	BB	219	DB	251	FB
28	1C	60	3C	92	5C	124	7C	156	9C	188	BC	220	DC	252	FC
29	1D	61	3D	93	5D	125	7D	157	9D	189	BD	221	DD	253	FD
30	1E	62	3E	94	5E	126	7E	158	9E	190	BE	222	DE	254	FE
31	1F	63	3F	95	5F	127	7F	159	9F	191	BF	223	DF	255	FF

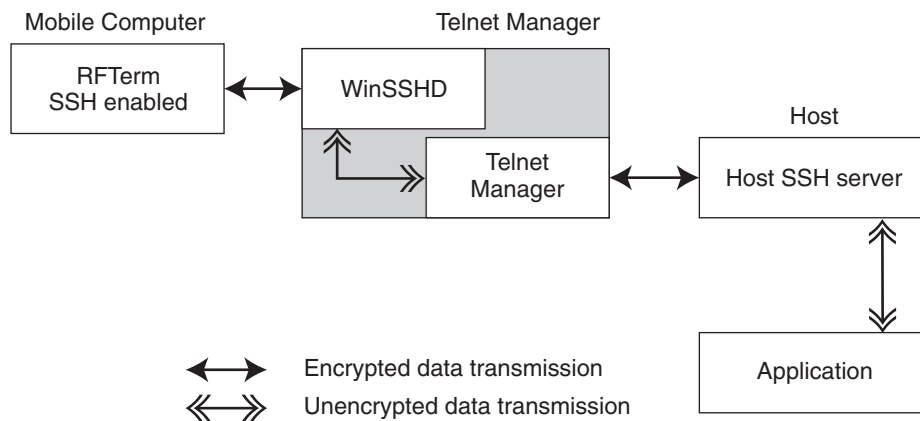
## SSH: Telnet Manager and RFTerm Case Study

### Introduction

This section provides an example of the configuration and interaction between RFTerm and Telnet Manager when SSH is enabled. This example assumes the user is familiar with network administration and has wired and wireless backbones in place. IP addresses and usernames/passwords provided in this case study are for example only and will vary based on the user's network configuration.

This example assumes the user has already installed and configured Telnet Manager, although this study will revisit some of the Telnet Manager and WinSSHD configuration options. This study also assumes the mobile computer has RFTerm installed and that the radio configuration utility has been properly configured to provide wireless network access.

The sample network in this case study is illustrated below. Note that in this example, the WinSSHD server and Telnet manager have the same IP address. The SSH host and end application are located on different PCs, but they could be installed on the same PC, if desired.



### Example Configuration

The configuration example in this case study covers:

- Microsoft Windows User Account and Firewall Configuration
- WinSSHD-LXETM1 Configuration
- Host Computer Configuration
- Telnet Manager Configuration
- RFTerm Configuration

#### Microsoft Windows User Account and Firewall Configuration

For more information on configuration options in this section, refer to the online Windows help feature or other documentation for Microsoft Windows.

##### Step 1: User Account

In this example, the Telnet Manager PC contains an account with user privileges as shown below:

- User name: User01
- Password: test1

If necessary, create a Windows user account.

##### Step 2: Open Port

Open port 22 in the Windows firewall. Port 22 is the default port for the incoming traffic to WinSSHD.

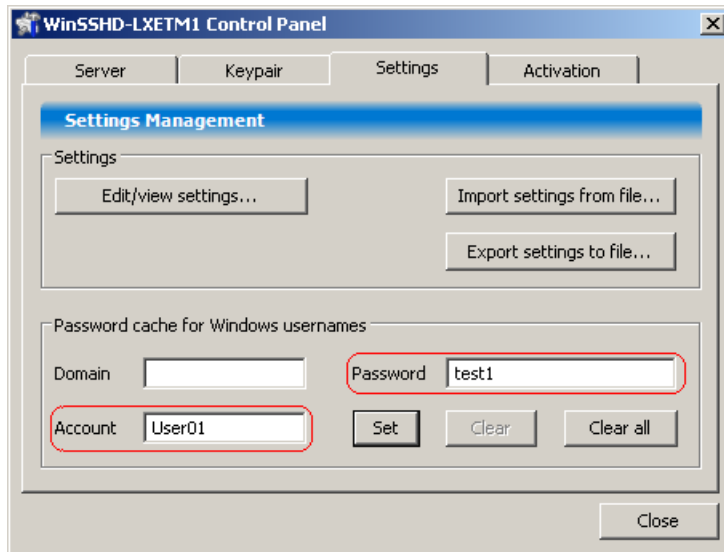
#### WinSSHD-LXETM1 Setup

For more information on configuring WinSSHD, refer to [Part 2: WinSSHD Setup](#) (page 20).

---

### Step 1: WinSSDH Settings

Start the WinSSHD-LXETM1 Control Panel and select the **Settings** tab.



- In the **Account** textbox, enter the username for the Windows account (see Microsoft Windows User Account and Firewall Configuration, earlier) to be used for Telnet Manager. In this example, the user account is User01.
- In the **Password** textbox, enter the password for the user account. In this example, the password is test1. Note that the password IS NOT displayed on this screen. WinSSHD masks the password entry with \*\*\*\*\*.

### Step 2: Save User Info

Click the **Set** button to save the username and password in the cache.

### Step 3: Edit Settings

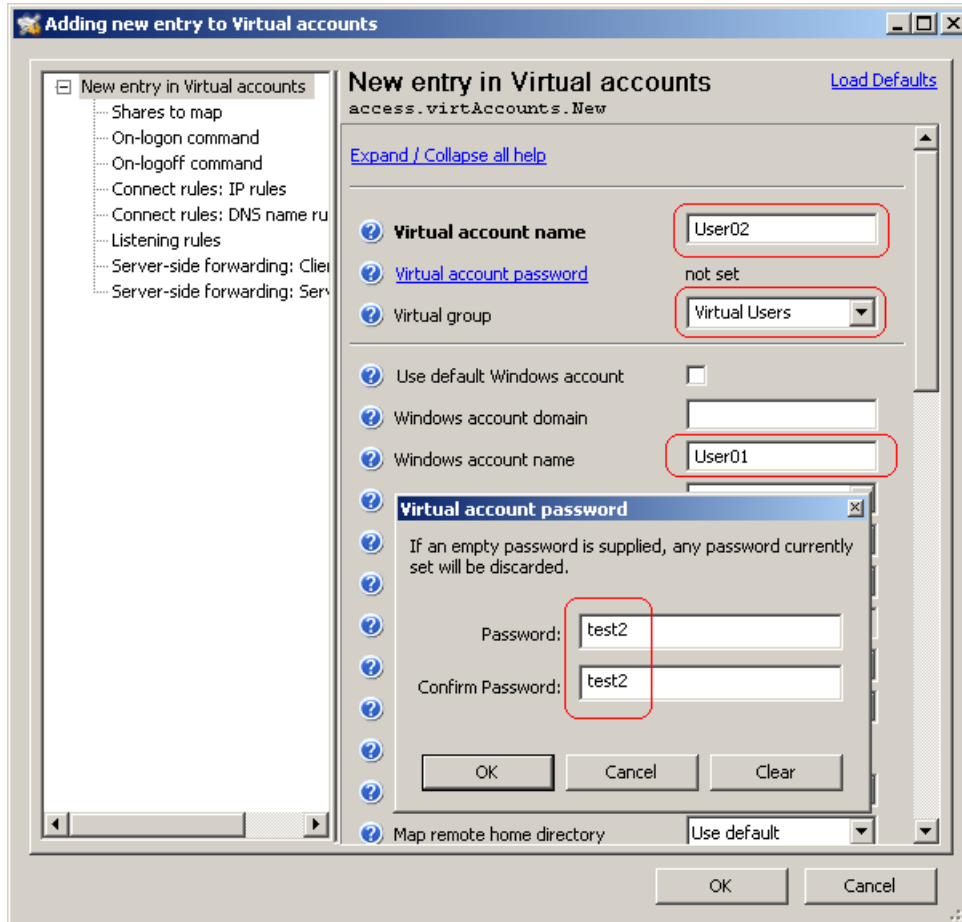
Click the **Edit/view settings...** button

### Step 4: Create Virtual Account

If a virtual account was not initially created, click the **Add** button. If there is an existing virtual account to be modified, select the appropriate virtual account and click the **Edit** button.

### Step 5: Configure Virtual Account

Configure the virtual account as shown.



- Enter a name for the virtual account. In this case, the Virtual account name is **User02**. This virtual account will be used for SSH authorization in RFTerm.
- Click to set the virtual account password. In this case, the password is **test2**. Note that the password IS NOT displayed on this screen. WinSSHD masks the password entry with \*\*\*\*\*.
- Set the **Virtual group** to Virtual users.
- Make sure **Use default Windows account** is unchecked.
- Enter the **Windows account name**. In this case, that is **User01** as specified in [Microsoft Windows User Account and Firewall Configuration](#) (page 121).

#### **Step 6: Save**

Click **OK** twice. This stores all configuration entries and returns to the WinSSHD-TM1 Control Panel **Settings** tab.

#### **Step 7: Export**

Click the **Export settings to file...** button. The file is saved with a **.wst** extension.

#### **Step 8: Start WinSSHD**

Click on the **Server** tab. Click the **Start WinSSHD** button.

### **Host Computer Setup**

Set up an SSH server on the host computer as specified for the SSH server installed on the host. In this example:

- The server is configured to use port 22.
- The username for the SSH server account on the Host computer is User03.
- The password for this account is test3.

## Telnet Manager Configuration

For more information on configuring Telnet Manager, refer to the Configuration Utility for the appropriate emulation:

- [ANSI Configuration Utility](#) (page 39)
- [IBM 3270 Configuration Utility](#) (page 69)
- [IBM 5250 Configuration Utility](#) (page 89)

In this example, the selected emulation is ANSI.

### Step 1: Global Configuration

Start TM1Config and select **Global Configuration**.

**Terminal Connection**

Allow unregistered terminals to connect

Port 1: 4000 Port 2: 4001 Port 3: 4002 Port 4: 4003

- Unregistered terminals are allowed to connect in this example. It won't be necessary to manually add each mobile device to Telnet Manager.
- Make sure the port that RFTerm uses is valid on the Global Configuration screen. In this case, port 4000 is to be used.

### Step 2: Restart Service

If any changes are made, save the current values and restart the service.

### Step 3: Master Template

Next, select **Client Registration > Master Template**.

**Host Connection (SSH shell)**

Name: 127.0.0.1 Port: 22

Connection timeout (seconds): 10

Connection Management: Always maintain connection (default)

Ssh

Off

Shell

Tunnel

Select Profile: [ ] **Edit/Create Profile**

Notice the following settings have been made:

- Notice that the SSH method has been selected. In this case, **Shell** is the SSH method. Note that Shell is only valid for ANSI.
- The **Name** and **Port** fields cannot be edited from this screen once SSH is enabled. Instead, they are entered in the SSH Profile screen, see below.

### Step 4: Create Profile

Click the **Edit/Create Profile** button.

In this example, a new profile is created. If a profile already exists, select that profile from the Select Profile list and proceed to the next step.

Select Profile

Select Profile  **Create New Profile**

[ ] Profile Name: Profile01

**Ssh Server:** Address: 127.0.0.1 Port: 22

**Authorization:**  **User+Pswd**

User/Password

User: User03

Password: \*\*\*\*\*

Advanced Settings

Keep Alive Ping Interval: 0 minutes

---

Select the Create New Profile option and enter a name for the profile in the textbox.

Enter the SSH Server information, IP Address and Port.

Enter the proper authorization credentials. In this case, a User Name and password are entered.

Click the **Save Profile** button and click the **X** to close the SSH settings screen.

### **Step 5: Save**

Telnet Manager is returned to the Client Registration Master Template.

Click the **Save current values** button.

### **Step 6: AutoLogin Scripts**

Complete and save any AutoLogin scripts

## **RFTerm Configuration**

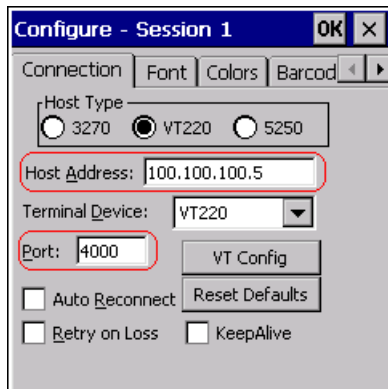
For more information on configuring RFTerm, refer to the RFTerm Reference Guide.

### **Step 1: Start RFTerm**

Start RFTerm if it is not already running on the mobile device.

### **Step 2: Configure Session**

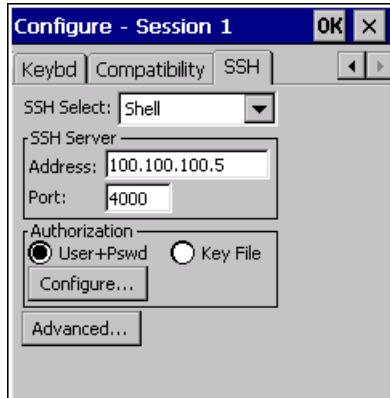
In this example, Session 1 is to be configured. Make sure Session 1 (S1) is selected. Click **Session > Configure** and make sure the **Connection** tab is selected.



- Select the proper **Host Type**. In this example, the host is **VT220**.
- Enter the IP address of the Telnet Manager in the **Host Address** box. If Telnet Manager and WinSSHD have different IP addresses, be sure to use the Telnet Manager IP address here.
- Enter the port in the **Port** box as set in the Telnet Manager Global Configuration screen. The Telnet Manager default ports are 4000, 4001, 4002 and 4003. In this example, port **4000** is used. Port 4000 has been opened in the Windows firewall and is specified on the Telnet Manager Global Configuration screen.

### **Step 3: Configure SSH**

Select the **SSH** tab.



- Make the type of SSH connection from the **SSH Select** list. In this example, Shell is used.
- Enter the IP address of the WinSSHD server in the **Address** box. If the Telnet Manager and WinSSHD have different IP addresses, be sure to use the WinSSHD IP address here.
- In the **Port** box, enter the port used to connect with the WinSSHD server. The default value is **22** and no change was made in WinSSHD to use another port.

#### **Step 4: User Authorization**

Click the **Configure** button.



- Enter the user credentials to log on to the Virtual User created during WinSSHD-TM1 configuration.
- In this example, **User** is **User02**
- The **Password** is **test2**. Note that the password IS NOT displayed on this screen. RFTerm masks the password entry with \*\*\*\*\*.

#### **Step 5: AutoLogin**

For ANSI only, select the **Auto Login** tab and check the box for **Auto Login enabled**.

#### **Step 6: Close Configuration**

Click **OK** to close all configurations screens. Make sure that **S1 (Session 1)** is selected on the Sessions tab. Select **Session > Connect** to connect to the selected session.

#### **Step 7: Data Processing**

Data transmission proceeds as follows:



- 
1. RFTerm encrypts data and transmits it securely to the WinSSHD server on the Telnet Manager PC.
  2. WinSSHD unencrypts the data and transmits it to the Telnet Manager.
  3. Telnet Manager forwards the data to the Host SSH server.
  4. The Host SSH server unencrypts the data and forwards it to the Host Application.

## **Other Examples**

### **SSH for RFTerm to Telnet Manager Only**

If the connection between Telnet Manager and the host/application is secure by design (for example a wired connection), it is possible to configure SSH for only the connection between RFTerm and Telnet Manager.

In this instance, follow the steps in [Example Configuration](#) (page 121) except:

1. On the Telnet Manager **Client Registration > Master Template**, do not check the **Use SSH** checkbox.
2. In the **Host** textbox, enter the IP address or domain name of the host.
3. It is not necessary to set up an SSH server on the host PC.
4. RFTerm must still be configured to use SSH and WinSSHD-LXETM1 must be properly configured for the incoming transmission.
5. Data transmission proceeds as follows:
  - RFTerm encrypts data and transmits it securely to the WinSSHD server on the Telnet Manager PC.
  - WinSSHD unencrypts the data and transmits it to the Telnet Manager.
  - Telnet Manager forwards the unencrypted data to host/application.

### **SSH for Telnet Manager to Host Only**

If it is not necessary to maintain an SSH connection between the mobile computers running RFTerm but it is necessary to have an SSH connection from Telnet Manager to the host, follow the steps in [Example Configuration](#) (page 121) except:

1. Do not check the Use SSH option in RFTerm.
2. It is not necessary to configure WinSSHD.
3. The SSH server on the host must be configured for the SSH transmission.
4. On the Telnet Manager **Client Registration > Master Template**, check the **Use SSH** checkbox. And enter the profile name and encryption keys.
5. Data transmission proceeds as follows:
  - RFTerm sends unencrypted data to Telnet Manager.
  - Telnet Manager forwards the encrypted to the Host SSH server.
  - The Host SSH server unencrypts the data and forwards it to the Application.

## **SSH Help**

To diagnose problems with the SSH configuration, be aware of the following features available:

On the **Server** tab of the WinSSHD-LXETM1 control panel, click the **View Windows Event Log...** button to view entries made to the event log. Entries labeled as WinSSHD-LXETM1 may help narrow authentication issues.

Telnet Manager can be configured to provide more information to be written to the debug log. See [sSetDBLevel x](#) (page 34) for more details.





Honeywell Scanning & Mobility  
9680 Old Bailes Road  
Fort Mill, SC 29707

[www.honeywellaidc.com](http://www.honeywellaidc.com)