Wavelink TermProxy
Version 4.0 User Guide

tp-ug-20070608-01

Revised 6/8/07

Wavelink Corporation
6985 South Union Park Avenue, Suite 335
Midvale, Utah 84047
Telephone: (801) 316-9000
Fax: (801) 316-9099
Email: customerservice@wavelink.com
Website: http:\\www.wavelink.com

Email: sales@wavelink.com

Table of Contents

Chapter 1: Introduction 5
Document Assumptions 5
Document Conventions 6
Overview of TermProxy 6
Functional Overview of TermProxy 7
Supported Connections 8
TermProxy Run-Time Options 8
TermProxy Features 9

Chapter 2: Installation 11
Obtaining the TermProxy Installation 11
Windows 11
AS/400 11
Linux 11
AIX 12
Installation Requirements. 12
Windows Requirements 12
AS/400 Requirements 13
Linux Requirements 14
AIX Requirements 14
Installing TermProxy. 14
Installing TermProxy on Windows 14
Installing TermProxy on the AS/400 Server 18
Installing TermProxy on Linux 21
.Installing TermProxy on AIX 22
Reinstalling TermProxy on the AS/400 22
Uninstalling TermProxy 24
Uninstalling TermProxy on Windows 24
Uninstalling TermProxy on the AS/400 25
Uninstalling TermProxy on Linux 26
Uninstalling TermProxy on AIX 26

Chapter 3: Configuration 27
Configuration Overview. 27
Accessing the Configuration Page. 27
Configuration Components 29
Default TermProxy Configuration 30
TermProxy Configurations. 31
Adding Entries 31
Configuration Format 31
Proxyservice 32
Hostservice 33
Loglevel 36

HTTPserver 37
Using Comment Delimiters 38
Configuring Reconnect Strings 39
5250 Reconnect String Examples 39
3270 Reconnect String Examples 40
VT Escape Sequence 40
Translating Table Statements 42
Validating Configuration Entries 42
Saving and Restarting Configurations 43
Sample Configurations 43
Sample Configuration 1 43
Sample Configuration 2 44

Chapter 4: Using TermProxy 47
TermProxy Functionality 47
Using TermProxy with Telnet Client. 48
Initiating a Telnet Session with TermProxy 49
Configuring the Telnet Host Profile 49
Host tab 49
TermProxy 1 Tab 51
SSL/TLS Encryption and Verification 56
Installing the SSL/TLS Support Utility on the PC 56
Deploying the SSL/TLS Support Utility to the Mobile Device . . 56
Enabling SSL/TLS Support 58
Enabling SSL/TLS Verification 58
Creating a New Certificate 60
Inserting Verification Certificates 61
Removing a Certificate 62
SSH Encryption and Verification 62
Custom Encryption 63
TermProxy Web Interface Operations. 63
Accessing the TermProxy Web Interface 64
Viewing the TermProxy Readme File 64
Viewing the TermProxy Release Notes 64
Restarting TermProxy 65
Logging and Data Capture 66
Overview 67
TermProxy Logging Levels 67
Setting the Logging Level 68
Enabling Data Capture 70
Viewing Files 71
Refreshing Files 72
TermProxy HTTP settings 73
Overview of TermProxy HTTP settings 73
Changing TermProxy HTTP Settings 74
Viewing TermProxy Status and Sessions 75

Viewing Session Status 75
Suspending a Session 78
Viewing Session List 78
Running TermProxy as a Service 79
Using TermProxy Command Line Switches 80
Installing and Uninstalling the TermProxy Service 82
Starting or Stopping the TermProxy Service 82

Appendix A: Implementation Scenarios 85
Scenario 1: Multiple Clients to a Single Host 85
Scenario 2: Multiple Clients to Multiple Hosts 86
Scenario 3: Multiple Clients to Proxy Server/Host 87

Appendix B: Running TermProxy as a Console Application (Win 32 only) 89
Launching TermProxy 89
Using TermProxy Command-Line Switches 90
Using TermProxy Console Commands 92
Closing TermProxy 93
Uninstalling TermProxy 94

Appendix C: Wavelink Contact Information 95

Glossary 97

Index 101

Chapter 1: Introduction

The purpose of this document is to provide an explanation of the installation, configuration, and use of TermProxy.

This chapter provides the following information:

- Document Assumptions
- Document Conventions
- Overview of TermProxy

Document Assumptions

This document is intended for IT professionals and assumes the following level of knowledge:

- An understanding of TCP/IP, including IP addressing, port numbers, and using Telnet for terminal emulation.
- Basic knowledge of the function of proxy services.
- Experience using Telnet on mobile devices for terminal emulation.

Document Conventions

This document uses the following typographical conventions:

`Courier New`	Any time you interact with an option (such as a button) or type specific information into a text box (such as a file name), that option appears in the `Courier New` text style. This text style is also used for any keyboard commands that you might need to press. Examples: Click `Next` to continue. Press `CTRL+ALT+DELETE`.
Bold	Any time this document refers to an option, such as descriptions of different options in a dialog box, that option appears in the **Bold** text style. Examples: Click `Open` from the **File** Menu.
Italics	Any time this document refers to another section within the document, that section appears in the *Italics* text style. This style is also used to refer to the titles of dialog boxes. Example: See *TermProxy Features* on page 9 for more information. The *Host Profiles* dialog box appears.

Overview of TermProxy

TermProxy is designed to extend the life of sessions between clients and hosts. Under normal operating circumstances, a client might go idle or enter power saving mode that prematurely terminates the session between the client and the host. A prematurely terminated session can cause a variety of

problems, including the loss of productivity. This section provides the following information:

- Functional Overview of TermProxy
- Supported Connections
- TermProxy Run-Time Options
- TermProxy Features

Functional Overview of TermProxy

TermProxy acts as an intermediary or proxy server between a client and a host, maintaining an established session between the two even though the client might go idle or otherwise terminate the session. The following steps illustrate the process:

1. The client establishes a session with the proxy server. (This is called the client-proxy session.)
2. The proxy server establishes a session with the host on behalf of the client and keeps track of the session information. (This is called the proxy-host session.)
3. The proxy server maintains the proxy-host session, even though the client-proxy session might go idle or dead. (You define the amount of time that the proxy server maintains the proxy-host session after the client-proxy session has gone idle or has otherwise been terminated.)
4. When a client re-connects after having been idle or having otherwise terminated the session, the proxy server sends the client the session information and the client continues the session as if the session had never been terminated. Block-mode emulations, such as 5250 and 3270, require a reconnect string. Character-mode emulations, such as VT100 and VT220, do not require a reconnect string.

The following figure provides a conceptual overview of this process.

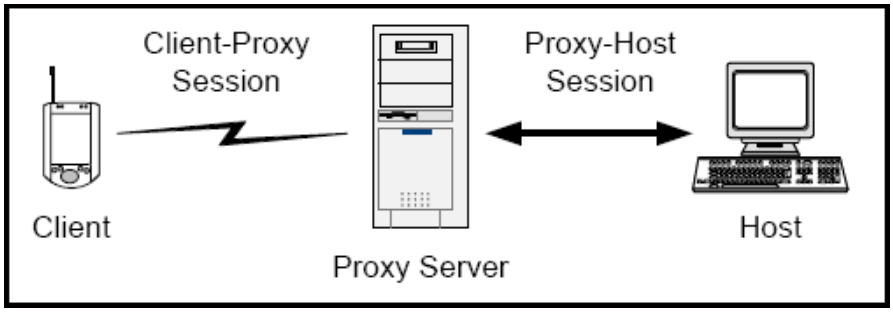

Figure 1-1. *TermProxy Process*

Supported Connections

TermProxy supports 10,000 concurrent socket connections. Because each connection from the client to the host through the proxy server requires two sockets (one client-proxy socket and one proxy-host socket), TermProxy can support a maximum of 5000 concurrent client Telnet sessions.

The number of concurrent connections that TermProxy supports is resource-dependent. If you plan on supporting a large number of clients (up to 5000), ensure that the host system meets the proper TermProxy specifications. The host system requirements appear in *Installation Requirements* on page 7.

TermProxy and the Wavelink Telnet Client support multiple terminate-on-exit options that may help free up unused or idle connections. These terminate options are: `On Exit`, `Never on Exit`, `Always on Exit`, and `On Network Error`.

TermProxy Run-Time Options

You have the option of installing and running TermProxy as one of the following:

- **Win32 installation**. This installs TermProxy as a Windows service or a standalone application.
- **OS/400 installation**. This installs TermProxy as a batch job using the WAVELINKTP user profile.
- **Linux installation.** This installs TermProxy as a daemon or a standalone application.

- **AIX installation.** This installs TermProxy as a daemon or a standalone application.

TermProxy Features

The following list describes the additional features that TermProxy offers:

- **Web Interface.** TermProxy offers a web interface that allows you to configure TermProxy, view log files, view data captures, delete client-proxy or proxy-host sessions, and review a comprehensive status section for each proxyservice. Sessions with the TermProxy web interface can be encrypted using SSL or SSH. A user name and password are required to access the web interface.

- **Restart Capability.** TermProxy provides a feature that allows you to restart TermProxy. Restarting TermProxy clears all active sessions.

- **Suspend/Resume Host Services.** TermProxy provides a feature that allows you to suspend additional connections to a proxyservice. All current connections remain functional, but new connections are denied until you resume the proxyservice.

- **Retrieve/Display IBM Workstation ID.** You can configure TermProxy to retrieve the IBM workstation ID from the data stream of a client. The workstation ID displays with the IP address of the client in the TermProxy interface. (This applies only to clients that are attempting to connect to an IBM AS/400 system.) TermProxy provides additional security with its handshaking protocol. Only those hosts specified for a given proxyservice are allowed to gain access to the host unless an adhoc proxy service is configured.

- **Multiple Proxy Sessions per Client.** TermProxy supports multiple proxy sessions with a single mobile device.

- **SSL Support.** TermProxy supports SSL encryption and verification for connections to the web interface and client-proxy connections.

- **SSH Support.** TermProxy supports SSH encryption and verification for proxy-host connections.

- **Extended Platform Support.** TermProxy is available for Microsoft Windows 2000, Windows 2000 server, Windows 2003 server, Windows XP

Professional, Windows XP Professional Service Pack 2, IBM AS/400 with either V5R2 or V5R3 OS versions, Linux, and AIX.

- **Data Capture Filter.** You can configure TermProxy to capture data from a single client, from multiple clients, or from all clients. Captured data is stored in a text file on the host system. You can view the text file either manually or through the TermProxy web interface.

Chapter 2: Installation

This chapter provides the following information:

- Obtaining the TermProxy Installation
- Installation Requirements
- Installing TermProxy
- Uninstalling TermProxy

Obtaining the TermProxy Installation

This section provides information about obtaining the files that are required to install TermProxy on the following operating systems:

- Windows
- AS/400
- Linux
- AIX

Refer to *Appendix C: Wavelink Contact Information* on page 95 for Wavelink Customer Service contact information.

Windows

All files required to install and operate TermProxy are included in an InstallShield executable. You can obtain this executable from www.wavelink.com, or by contacting Wavelink Customer Service.

AS/400

The OS/400 TermProxy installation is distributed via CD. To obtain the AS/400 installation CD, contact Wavelink Customer Service.

Linux

The Linux installation is a `.rpm` file that can be obtained from www.wavelink.com, or by contacting Wavelink Customer Service.

AIX

The AIX installation is a `.rpm` file that can be obtained from www.wavelink.com, or by contacting Wavelink Customer Service.

Installation Requirements

This section provides information about the minimum and recommended requirements for the system that will host TermProxy. The following information is included:

- Windows Requirements
- AS/400 Requirements
- Linux Requirements
- AIX Requirements

Windows Requirements

The host system should meet the following requirements:

- Microsoft Windows 2000/XP Professional, Windows 2003 or 2000 Server
- Intel Pentium 4 2.4 GHz (or equivalent) Processor
- 512 MB RAM if you plan to use less than 1000 Telnet clients
- 1GB RAM if you plan to use more than 1000 Telnet clients
- 50 MB disk space

NOTE Each client-to-host connection through TermProxy requires approximately 64 KB of RAM per session.

NOTE Wavelink Corporation recommends that if you are supporting more than 1000 clients, you use a dedicated server to host TermProxy.

NOTE TermProxy requires additional hard disk space to support the log file. For additional information about the TermProxy log file, see *Overview of TermProxy Logging* on page 66.

NOTE Out of the box, the Windows 2000/XP operating systems will only support about 1000 TermProxy sessions. To increase the number, create the following setting in the Windows registry:

```
[HKLM]/SYSTEM/CurrentControlSet/Services/Tcpip/Parameters
MaxUserPort=65534    (DWORD)
```

This allows WinSock to work with a larger pool of ephemeral ports.

AS/400 Requirements

The host system should meet the following requirements:

- OS/400 V5R2 or higher with IFS
- AS/400 Processor and memory
- 70 MB disk space
- Multiply interactive processor requirement by .5 and add this to the interactive processor requirement
- Double the interactive memory requirement

NOTE Contact your IBM representative to determine what your interactive requirements are based upon your needs.

NOTE Each AS/400 client-to-host connection through TermProxy requires approximately 128 KB of RAM.

Linux Requirements

The host system should meet the following requirements:

- Intel Pentium 4 2.4 GHz (or equivalent) Processor
- 512 MB RAM if you plan to use less than 1000 Telnet clients
- 1GB RAM if you plan to use more than 1000 Telnet clients
- 50 MB disk space

AIX Requirements

The host system should meet the following requirements:

- 512 MB RAM if you plan to use less than 1000 Telnet clients
- 1GB RAM if you plan to use more than 1000 Telnet clients
- 50 MB disk space

Installing TermProxy

This section provides instructions for installing TermProxy. The following information is provided:

- Installing TermProxy on Windows
- Installing TermProxy on the AS/400 Server
- Installing TermProxy on Linux
- .Installing TermProxy on AIX
- Reinstalling TermProxy on the AS/400

Installing TermProxy on Windows

This section contains information about installing TermProxy for use on a Windows machine.

To install TermProxy:

1 Obtain and transfer the TermProxy installation program to the target host system.

NOTE To obtain the TermProxy installation program, contact Wavelink Customer Service. Refer to *Appendix C: Wavelink Contact Information* on page 97 for more information.

---

2 Launch the InstallShield executable.

The *Wavelink TermProxy InstallShield Wizard* appears.

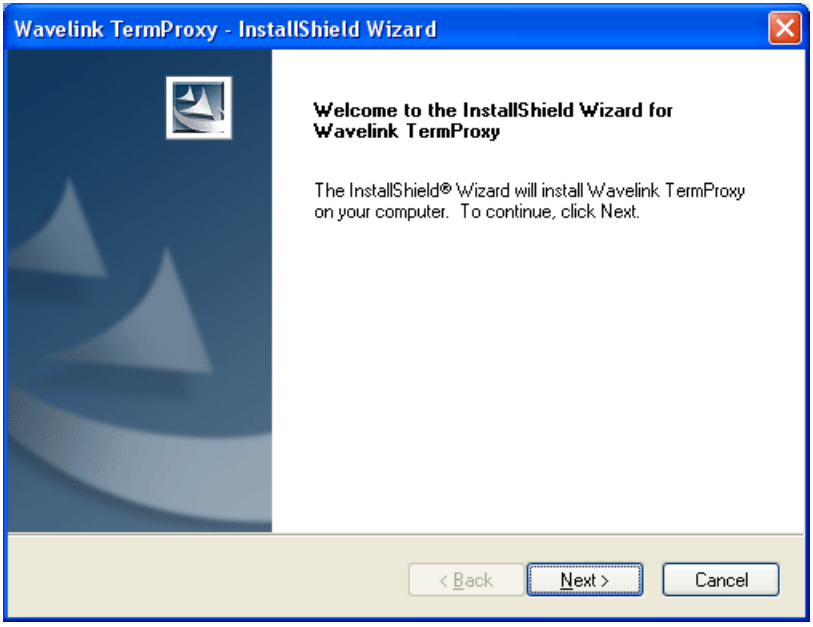

Figure 2-1. *InstallShield Wizard*

3 Click `Next`.

The *License Agreement* dialog box appears.

4 Enable the **I accept the terms of the license agreement** option and click `Next`.

NOTE If you do not accept the terms of the license agreement, you will not be able to continue the installation.

The *Choose Destination Location* dialog box appears.

5 Click `Next` to accept the default installation location, or click `Change...` to navigate to a folder of your choice. After you select an installation folder, click `Next` to continue the installation process.

The *Target Host* dialog box appears.

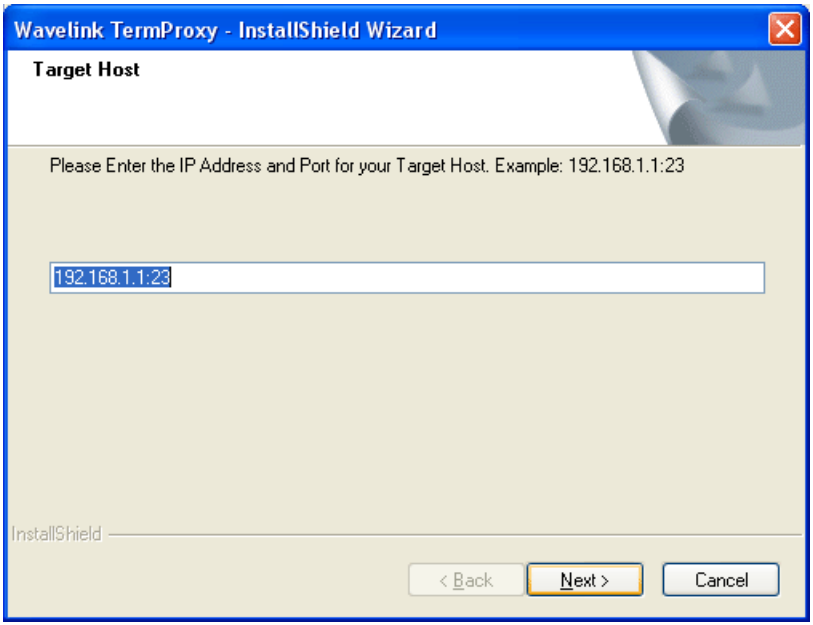

Figure 2-2. *Target Host Dialog Box*

6 In the text box, enter the IP address and the TCP port of a host server using the `IP address:Port` format.

For example:
`192.168.1.1:23`

7 Click `Next`.

The *TermProxy Web Server Port* dialog box appears.

8 In the text box, enter the web server port number. The web server port number is the TCP port on which the host system will accept connections to the TermProxy web interface.

NOTE The default port number is 4428.

---

9 Click `Next`.

The *TermProxy Web Server Username and Password* dialog box appears.

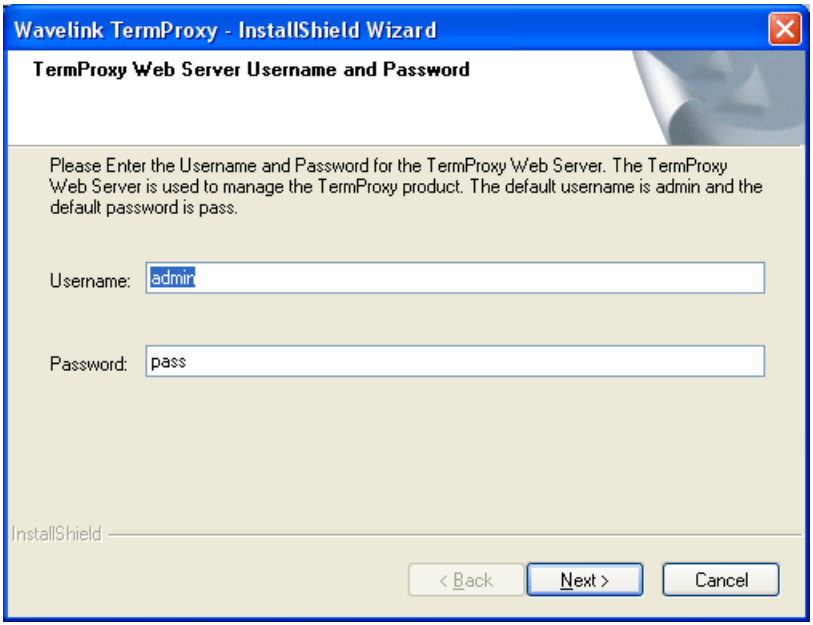

Figure 2-3. *TermProxy Web Server Username and Password Dialog Box*

10 Enter a user name for the web server in the **Username** text box.

NOTE The default user name is “admin”.

---

11 Enter a password for the web server in the **Password** text box.

NOTE The default password is “pass”.

12 Click `Next`.

The *TermProxy Install Complete* dialog box appears.

13 If desired, enable the **Launch Readme** and **Start Service** checkboxes and click `Finish`.

If you enabled the **Start Service** checkbox, the installation launches a web browser and prompts you to enter the username and password to access the TermProxy web server.

Installing TermProxy on the AS/400 Server

This section contains information about installing TermProxy for use on an AS/400 server.

NOTE You must have Qsecofr authority to install TermProxy on the AS/400 server.

To install TermProxy on the AS/400:

1 Insert the installation CD into the AS/400.

NOTE To obtain the AS/400 installation CD, contact Wavelink Customer Service. Refer to *Appendix C: Wavelink Contact Information* on page 97 for more information.

2 Connect to an AS/400 Telnet session.

Figure 2-4. *AS/400 Main Menu*

3 At the command prompt, enter `LODRUN DEV(OPT01)` and press `Ctrl-Enter`.

The *Wavelink End User License Agreement* screen appears.

4 Enter `Y` and press `Ctrl-Enter` to agree to the licensing information.

NOTE If you do not agree to the licensing information, you will not be able to complete the installation process.

The *Authority Required to Install TermProxy* screen appears.

5 Press `Ctrl-Enter`.

The installation verifies your Qsecofr authority. The install will abort with a message if the Qsecofr authority is not found. If the Qsecofr authority is found the *TermProxy Web Server Configuration* screen appears.

6 Press `Ctrl-Enter`.

The configuration editor appears.

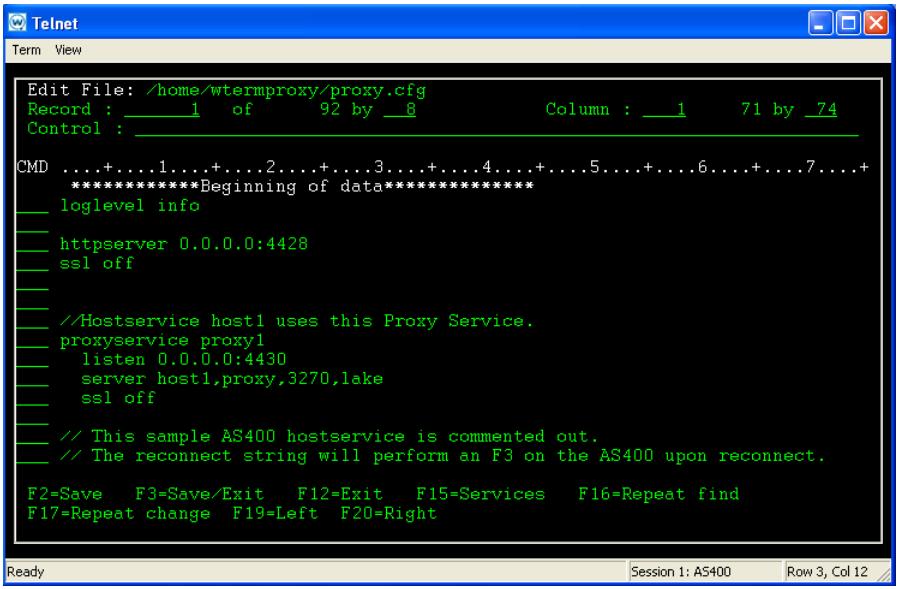

Figure 2-5. *AS/400 Configuration Editor*

7 If desired, edit the configuration file and press `F3`.

-Or-

Press `F3` to keep the configuration file in the default state.

8 Press `F3` again to exit the editor.

The *Starting TermProxy* screen appears, asking if you want to start TermProxy now or later.

9 Enter `Y` and press `Ctrl-Enter` to start TermProxy.

The *TermProxy Installation Complete* screen appears.

10 Press `Ctrl-Enter` to complete the installation and return to the command line.

NOTE A WTPINST library is also saved to the AS/400 when TermProxy is installed. This library contains a few very small installation objects. After a successful TermProxy installation, you can delete the WTPINST library, if desired.

Installing TermProxy on Linux

This section contains information about one method for installing TermProxy on a Debian and Non-Debian Linux operating system.

NOTE There are alternative methods for installing TermProxy on Linux. You may use a different installation method if desired.

To install TermProxy on a Debian Linux distribution:

1 Download the `.rpm` installation file.

2 Enter the following commands at the terminal:

```
alien --scripts termproxyfile.rpm
alien -i --scripts termproxyfile.deb
```

TermProxy is installed on the host system.

3 To start TermProxy, use the following command:

```
/etc/init.d/termproxy start
```

4 To stop TermProxy, use the following command:

```
/etc/init.d/termproxy stop
```

To install TermProxy on a Non-Debian Linux distribution:

1 Download the `.rpm` installation file.

2 Enter the following command at the terminal:

```
rpm -i [filename]
```

-Or-

If you are using a GUI, double-click on the installation file.

TermProxy is installed on the host system.

3 To start TermProxy, use the following command:

```
/etc/init.d/termproxy start
```

4 To stop TermProxy, use the following command:

```
/etc/init.d/termproxy stop
```

.Installing TermProxy on AIX

This section contains information about one method for installing TermProxy on an AIX operating system.

NOTE There are alternative methods for installing TermProxy on AIX. You may use a different installation method if desired.

To install TermProxy on AIX:

1 Download the `.rpm` installation file.

2 Enter the following command at the terminal:

```
rpm -i [filename]
```

-Or-

If you are using a GUI, double-click on the installation file.

TermProxy is installed on the host system.

Reinstalling TermProxy on the AS/400

The steps to reinstall TermProxy on the AS/400 are similar to the steps to install TermProxy on the AS/400. However, when you reinstall TermProxy, the installation application detects that a Wavelink TermProxy Library and WTermProxy IFS Directory already exist. You have options to either maintain or delete the existing library and directory.

To reinstall TermProxy on the AS/400:

1 Insert the installation CD into the AS/400.

2 Connect to an AS/400 Telnet session.

3 At the command prompt, enter `LODRUN DEV(OPT01)` and press `Ctrl-Enter`.

The *Wavelink End User License Agreement* screen appears.

4 Enter `Y` and press `Ctrl-Enter` to agree to the licensing information.

NOTE If you do not agree to the licensing information, you will not be able to complete the installation process.

The *Authority Required to Install TermProxy* screen appears.

5 Press `Ctrl-Enter`.

The installation verifies your Qsecofr authority. The install will abort with a message if the Qsecofr authority is not found. If the Qsecofr authority is found, the *Wavelink TermProxy Library Already Exists* screen appears.

6 Enter `Y` to overwrite the WTERMPROXY library or `N` to keep the existing WTERMPROXY library and abort the install, and press `Ctrl-Enter`.

The *WTermProxy IFS Directory Exists* screen appears.

7 Enter `Y` and press `Ctrl-Enter` to maintain the previous directory settings.

The configuration editor appears.

8 If desired, edit the configuration file and press `F3`.

-Or-

Press `F3` to keep the configuration file in the default state.

9 Press `F3` again to exit the editor.

The *Starting TermProxy* screen appears.

10 Enter `Y` and press `Ctrl-Enter` to start TermProxy.

The *TermProxy Installation Complete* screen appears.

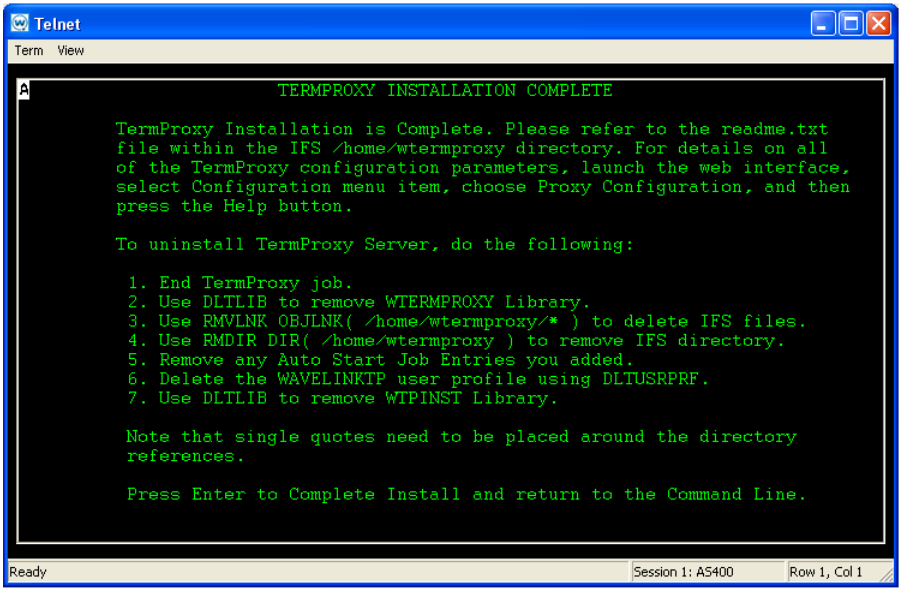

Figure 2-6. *AS/400 Installation Complete Screen*

11 Press `Ctrl-Enter` to complete the installation and return to the command line.

Uninstalling TermProxy

This section provides information about uninstalling TermProxy. The following information is included:

- Uninstalling TermProxy on Windows
- Uninstalling TermProxy on the AS/400
- Uninstalling TermProxy on Linux
- Uninstalling TermProxy on AIX

Uninstalling TermProxy on Windows

This section contains information about uninstalling TermProxy on a Windows machine.

To uninstall TermProxy:

1 On the host system, open the *Control Panel*.

2 Select `Add or Remove Programs`.

3 Locate **Wavelink Termproxy** and click the `Change/Remove` button.

4 Verify that you want to uninstall the program and click `Uninstall`.

TermProxy is uninstalled on the host system.

Uninstalling TermProxy on the AS/400

This section provides information about uninstalling TermProxy on the AS/400.

To uninstall TermProxy:

1 End the TermProxy job.

2 At the command line, enter `DLTLIB` to remove the WTERMPROXY library.

3 To delete the IFS files, enter the following command at the command line:

```
RMVLNK OBJLNK ('/home/wtermproxy/*')
```

4 To delete the IFS directory, enter the following command at the command line:

```
RMDIR DIR (/home/wtermproxy)
```

NOTE Place single quotes around the directory references.

---

5 Remove any Auto Start Job Entries you added.

6 At the command line, enter `DLTUSRPRF` to delete the WAVELINKTP user profile.

7 At the command line, enter `DLTLIB` to delete WTPINST library.

Uninstalling TermProxy on Linux

This section provides information about uninstalling TermProxy on a Linux operating system.

To uninstall TermProxy:

- Use the following command to uninstall the `.rpm` file:

  ```
  rpm -e --allmatches termproxy
  ```

  TermProxy is removed from the host system.

Uninstalling TermProxy on AIX

This section provides information about uninstalling TermProxy on an AIX operating system.

To uninstall TermProxy:

- Use the following command to uninstall the `.rpm` file:

  ```
  rpm -e --allmatches termproxy
  ```

  TermProxy is removed from the host system.

Chapter 3: Configuration

This section provides the following information:

- Configuration Overview
- Accessing the Configuration Page
- Configuration Components
- TermProxy Configurations
- Sample Configurations

Configuration Overview

This section provides an overview of the tasks involved in creating and modifying TermProxy configurations. The following list describes the tasks that are required to create or modify a TermProxy configuration.

1. Access the TermProxy Configuration page in the TermProxy web interface.
2. Use the configuration interface to create or modify the TermProxy configuration.
3. Validate your changes.
4. Save and restart TermProxy.

NOTE You can also modify the configuration of TermProxy in the `termproxy.cfg` file. However, it is recommended that you use the *TermProxy Configuration* page in the TermProxy web interface for all configuration modifications.

Accessing the Configuration Page

You can edit and modify the TermProxy configuration using the *TermProxy Configuration* page in the TermProxy web interface. The *TermProxy Configuration* page allows you to add proxyservices and hostservices, modify

the TermProxy web server connection information, and modify the logging level.

To access the configuration page:

1 Open a web browser and type the address and port of the TermProxy web server.

Example: `http://192.168.1.10:4428`

2 Enter the user name and password.

NOTE The default username is `admin` and the default password is `pass`.

---

3 Click `OK`.

The *TermProxy Main Menu* page appears.

4 Click `Configuration`.

The *Logging and Data Capture Settings* page appears.

5 In the left-channel navigation, click `Proxy Configuration`.

The *TermProxy Configuration* page appears.

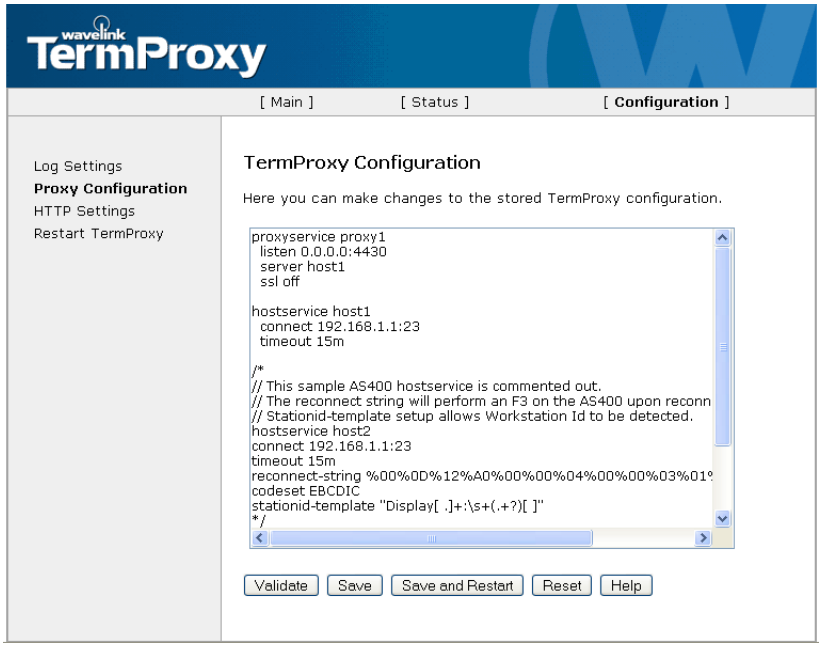

Figure 3-1. *TermProxy Configuration Page*

A sample configuration is provided as part of the installation and displays on the *TermProxy Configuration* page. Portions of this configuration are commented out. You can remove comments and modify the sample configuration to configure TermProxy for your system.

Configuration Components

The *TermProxy Configuration* page contains the following sections:

- **Proxyservice configuration information.** The first section defines the listen socket. This is the IP address and port number used by the proxyservice to listen for incoming mobile devices.
- **Hostservice configuration information**. The second section defines the host server socket. This is the IP address and port of the target host.
- **Log level information.** The third section defines the logging level.

- **HTTP server information**. The last section defines the web server listen socket. This is the IP address and port number that the TermProxy web server uses to listen for incoming administrative web sessions.

Default TermProxy Configuration

All TermProxy installations contain a default TermProxy configuration. The default configuration is as follows:

```
log level INFO

httpserver 0.0.0.0:4428
ssl off

/*

//hostservice host1 uses this Proxy Service
  proxyservice proxy1
  listen 0.0.0.0:4430
  server host1
  ssl off
  encryption passwordwouldgohere

//This sample AS400 hostservice is commented out.

//The reconnect string will perform an F3 on the AS400
upon reconnect.

//stationid-template setup allows Workstation ID to be
detected
hostservice host1
connect 192.168.1.1:23
timeout 15 m
reconnect-string
%00%0D%12%A0%00%00%04%00%00%03%01%01%33%FF%EF
codeset EBCDIC
stationid-template "Display [ .]+:\s+(.+?)[ ]
ssh off

*/
```

TermProxy Configurations

This section provides information about adding and modifying TermProxy configurations, validating configurations, and saving configurations. The following information is provided:

- Adding Entries
- Configuration Format
- Using Comment Delimiters
- Configuring Reconnect Strings
- Translating Table Statements
- Validating Configuration Entries
- Saving and Restarting Configurations

Adding Entries

For each proxyservice entry there must be at least one hostservice entry, but there can be many hostservices configured to work with a single proxyservice. The resources of the system on which you are running TermProxy determine the actual number of proxyservice and hostservice entries the TermProxy application can handle.

Each proxy entry requires 1 KB of RAM on the system that is hosting the TermProxy application.

Begin each parameter of the proxy entry on a new line. The TermProxy application ignores white space, so you can place as much white space as you would like before and after each parameter. You can also use as much space as you would like between proxy entries.

Parameters in the TermProxy configuration are not case-sensitive. You can use lower- and/or upper-case characters.

Configuration Format

This section contains information about the format and parameters of the following TermProxy configuration entries:

- Proxyservice
- Hostservice
- Loglevel
- HTTPserver

Proxyservice

Use the following format to enter a proxyservice entry in the TermProxy configuration:

```
proxyservice [proxyservicename]
   listen [ipaddr]:[port]
   server [hostservicename]:[hostserviceport]
   timeout [min]
   ssl [on | off]
```

The following table contains detailed information about each parameter in the proxyservice entry.

Parameter	Explanation
`proxyservice [proxyservice name]`	Specify a name for the proxy service. The name is used in the TermProxy user interface and log file. There is a 64 character maximum. This is a required parameter.
`listen [ipaddr:port]`	Specify the interface and port number on which the proxy server should listen for client connections, where `[ipaddr]` is the IP address of the interface and `[port]` is the port number on that interface. Use `0.0.0.0` to specify that the proxy server should listen for a specific port number on all local interfaces. For example, the entry `0.0.0.0:2301` instructs TermProxy to listen for client connections on port 2301 for all local interfaces on the TermProxy server. This is a required parameter.

Table 3-1: *Proxyservice Parameters*

`server [hostservice]`	Specify the hostservice names to be associated with a proxyservice. This parameter defines the host services that a client can access through this proxy service. The parameter value is a comma-separated list of host service names. Alternatively, an asterisk (*) can be specified as the host service name. TermProxy will then allow the client to establish sessions with arbitrary applications, whether they are configured with a hostservice statement or not. This is known as the unrestricted mode of operation. This is a required parameter.
`timeout [time]`	Specify the amount of time before TermProxy terminates the client-proxy session due to inactivity (also referred to as the client timeout). Specify a value of `0` to allow sessions to remain open indefinitely. An inactive client connection is one where the client has not sent or received data during the specified timeout interval. When TermProxy terminates a client connection, it will leave the proxy-host connection intact until the host timeout interval expires due to inactivity. A suffix can be used to indicate a time unit (1d=24h=1440m=86400s). The default suffix is m for minutes. This parameter is optional and will default to `24h` if not specified.
`ssl [on | off]`	Specify `on` to use the Secure Sockets Layer (SSL) protocol to communicate with the browser. TermProxy must be supplied with a valid server certificate and private key PEM files for SSL HTTP service to become operational. This parameter is optional and will default to `off` if not specified.
`encryption [passphrase]`	Type `encryption` and specify an encryption key to use custom encryption for client connections.

Table 3-1: *Proxyservice Parameters*

Hostservice

Use the following format to enter a hostservice entry in the TermProxy configuration:

```
hostservice [hostservicename]
   connect [ipaddr]:[port]
   ssh [on | off]
   ssh-verify [ssh-verify-on | off]
   timeout [min]
   reconnect-string [reconnect-string]
   undeliverable [Discard | Abort]
```

```
codeset [ASCII | EBCDIC]
stationid-template {regular expression]
translate-tohost [tablename]
translate-fromhost [tablename]
```

The following table contains detailed information about each parameter in the hostservice entry.

Parameter	Explanation
`hostservice [hostservicname]`	Specify a name for the host service. The name is used in the TermProxy user interface and log file. There is a 64 character maximum. This is a required parameter.
`connect [ipaddr:port]`	Specify the IP address and port of a target host. This is the interface and port number on which the proxy server should connect to the hostservice, where `[ipaddr]` is the IP address of the interface and `[port]` is the port number on that interface. A DNS name may be used in place of the IP address, but it must be followed by a colon and the port number. Example: app.host.com:1235. This is a required parameter.
`ssh [on | off]`	Specify either `on` or `off` to determine whether TermProxy uses SSH encryption for the proxy-host session.
`ssh-verify [ssh-verify on | off]`	Specify either `on` or `off` to determine whether to allow client-host connections when the public key does not match the expected key. If `off` is specified, the client-host connection will be allowed and warning messages will be sent to the client.
`timeout [min]`	Specify the amount of time before TermProxy terminates the proxy-host session. Specify a value of `0` to allow sessions to remain open indefinitely. This time begins once the client-proxy connection closes (after the client timeout expires). A suffix can be used to indicate a time unit (1d=24h=144=m=86400s). This parameter is optional and will default to `15m` if not specified.

Table 3-2: *Hostservice Parameters*

Parameter	Explanation
`reconnect-string [string]`	Specify a reconnect string, where `[string]` is the reconnect string. Reconnect strings entered within a Telnet Client host profile take precedence over reconnect strings configured using the TermProxy web interface. If specified, this string will be sent to the host application over the existing host connection when a client reestablishes a connection with TermProxy. You can specify any sequence of bytes in the reconnect string. Use quoting and/or escaping if necessary. Refer to *Configuring Reconnect Strings* on page 39 for more information. A reconnect-string is required for 5250/3270 applications.
`reconnect-buffer [size]`	Specify a value to determine the maximum amount of host-to-client data (in byes) that will be saved when a client reestablishes a connection with TermProxy. This option is only available if no reconnect-string is specified.
`undeliverable [DISCARD | ABORT]`	Specify either `DISCARD` or `ABORT` for sessions with a host connection, but no current client connection. `DISCARD` will delete unsolicited outbound data sent by the host application. `ABORT` will terminate the host connection. This parameter is optional and will default to `DISCARD` if not specified.
`codeset [ASCII | EBCDIC]`	Specify `ASCII` or `EBCDIC` to determine how TermProxy searches the application data for a stationid and how it presents capture file records. Select `EBCDIC` when using 5250 and the stationid-template. This parameter defaults to `ASCII` if not specified.
`stationid-template [regular expression]`	Specify the stationid-template. The stationid-template serves a very narrow purpose. It extracts the workstation ID from the initial outbound screen buffer of an IBM AS/400 Telnet server session and presents the ID in the active session list, alongside the client IP address. The search pattern must be in the form of a regular expression containing a single tagged expression. Example: `Display [ .]+:\s+(.+?)[ ]` This is an optional parameter and configured only with the 5250.

Table 3-2: *Hostservice Parameters*

Parameter	Explanation
`translate-to host [tablename]`	TermProxy provides a simple byte-replacement mechanism for the inbound data stream. To use this feature, you must define one or more mapping tables and reference the tables through the translate-tohost keywords. Refer to *Translating Table Statements* on page 42 for more information. This parameter is optional and defaults to `No translation` if not specified.
`translate-fromhost [tablename]`	TermProxy provides a simple byte-replacement mechanism for the outbound data stream. To use this feature, you must define one or more mapping tables and reference the tables through the translate-fromhost keywords. Refer to *Translating Table Statements* on page 42 for more information. This parameter is optional and defaults to `No translation` if not specified.

Table 3-2: *Hostservice Parameters*

Loglevel

Use the following format to enter a loglevel entry in the TermProxy configuration:

```
loglevel [preferred default logging level]
```

The following table contains detailed information about the loglevel entry.

Parameter	Description
`loglevel [`*`preferred default logging level`*`]`	Specify the log level. The log level controls the amount of data TermProxy writes into the log file. The information stored in the log file can be useful for trouble-shooting and auditing purposes. The log level allows you to manage the amount of collected data in order to control the overhead storage. This configuration setting is meant to be the 'normal' setting for the day-to-day operation. The *Logging and Data Capture Settings* page in the TermProxy Web interface allows you to temporarily change that level setting. The following is a list of the log level settings. The parenthesized numbers are numeric equivalents that can be used in place of the mnemonics. CRITICAL (1) Catastrophic error logging only ERRORS (2) Errors only WARNING (3) Errors and warnings INFO (4) Errors, warnings, informational DEBUG (5) Trouble-shooting mode VERBOSE (6) All errors, warnings, and trouble-shooting information from other modes
`capture [`*`on`*` | `*`off`*`]`	Specify either `on` or `off` to determine whether proxy communication data is captured.
`clear [`*`on`*` | `*`off`*`]`	Specify either `on` or `off` to determine whether the data capture file is emptied when TermProxy starts or restarts.
`restart [`*`time`*`]`	Specify a comma-delimited list of times that TermProxy will automatically restart. Enter times using the following format: `HH:MM[a|p]`. If there is no `a` (A.M.) or `p` (P.M.) indicated, the time is assumed to be in 24-hour format. Specify a weekly time by preceding the time with the day of the week. Examples: `10:00P, 06:00A, MONDAY22:30` This is a required parameter.

Table 3-3: *Loglevel Parameters*

HTTPserver

Use the following format to enter an httpserver entry in the TermProxy configuration:

```
httpserver [ipaddr]:[port]
  ssl [on | off]
```

The following table contains detailed information about the httpserver entry.

Parameter	Description
`httpserver [ipaddr:port]`	Specify the IP address and port to which the TermProxy HTTP service binds itself. You would normally specify the ANY/ALL address and a free port number. Example: `0.0.0.0:4428` Alternatively, you could restrict access to the HTTP interface to the local machine. Example: `httpserver localhost:4428`. TermProxy requires both an httpserver statement and a userid/password specification before it will activate the HTTP service. This is a required parameter.
`ssl [on | off]`	Specify `on` to use the Secure Sockets Layer (SSL) protocol to communicate with the browser. TermProxy must be supplied with a valid server certificate and private key PEM file for SSL HTTP service to become operational. The directory where the TermProxy service resides contains a default servercert.pem and serverkey.pem file. Use `https://[IP address of TermProxy Web server]:[Port of TermProxy Web server]`. This parameter is optional and will default to `off` if not specified.

Table 3-4: *Httpserver Parameters*

Using Comment Delimiters

You must comment out non-essential text in the configuration. You must use the appropriate comment delimiters (that is, characters) to comment out text. The TermProxy application ignores any text in the configuration that you have commented out. You can use comment delimiters to insert notes and other useful information.

NOTE You must place white space before and after all comment delimiters. A single space is enough, but there is no limit to the amount of space that you may use.

Use the following comment delimiters to comment out non-essential text in the TermProxy configuration:

- **Double-slash (//).** Use a double-slash to comment out the remaining part of a single line of text.

  For example:

  ```
  Listen 0.0.0.0:2301  // all IP connections to port 2301
  ```

  The TermProxy application will ignore the last part of the line, which reads "`all IP connections to port 2301`".

- **Slash asterisk-asterisk slash (/* */).** Use the slash asterisk-asterisk slash to comment out a section of text. Place the slash-asterisk (/*) at the beginning of the section of text. Place the asterisk-slash (*/) at the end of the section of text.

  For example:

  ```
  /*

  This configuration file is for all clients that are
  using TermProxy to connect to hosts 10.22.15.121 and
  10.22.122.122.

  All clients that want to connect to host 10.22.15.123
  should connect to the host through TermProxy that is
  running on server 10.22.15.120.

  */
  ```

  You might place the sample text before a proxyservice entry in the configuration. The TermProxy application would ignore all of the lines of text that are enclosed in the (/* */) comment delimiter.

Configuring Reconnect Strings

When you enter a `[string]` value, you must place a `%` character before each hex code value. Each hex code character is represented by a two-digit number.

5250 Reconnect String Examples

The following are examples of the `[string]` variable in the reconnect-string parameter of a hostservice entry:

- To send an `F24` upon reconnect (EBCDIC BC before FFEF):

```
%00%0D%12%A0%00%00%04%00%00%03%01%01%BC%FF%EF
```

- To send a reconnect command for the 5250 `F3` key (EBCDIC 33 before FFEF):

  ```
  %00%0D%12%A0%00%00%04%00%00%03%01%01%33%FF%EF
  ```

- To send a reconnect command for the 5250 `ENTER` key (EBCDIC F1 before FFEF):

  ```
  %00%0D%12%A0%00%00%04%00%00%03%01%01%F1%FF%EF
  ```

These strings represent all the necessary 5250 Telnet data needed to send the respective aid key.

3270 Reconnect String Examples

The following are examples of the `[string]` variable in the reconnect string parameter of a hostservice entry:

- To send a reconnect command for the 3270 `F11` key:

  ```
  %7B%C8%F9%FF%EF
  ```

- To send a reconnect command for the 3270 `F4` key:

  ```
  %F4%C8%F9%FF%EF
  ```

- To send a reconnect command for the 3270 `ENTER` key:

  ```
  %7D%C8%F9%FF%EF
  ```

- To send a reconnect command for the 3270 `F1` key:

  ```
  %F1%C8%F9%FF%EF
  ```

VT Escape Sequence

The following are examples of the [*string*] variable in the reconnect string parameter of a host service entry:

- To send a reconnect command for the VT100 or VT220 F3 key:

  ```
  %1BOR
  ```

  This returns you to a menu screen upon reconnect.

- To send a reconnect command for the VT100 or VT220 F11 key:

  ```
  %1B[23~
  ```

  This calls a new screen upon reconnect.

The following Hex codes can be used as reconnect strings.

Hex Value	Character	
%00	Ctrl-A	
%01	Ctrl-B	
%02	Ctrl-C	
%03	Ctrl-D	
%04	Ctrl-D	
%05	Ctrl-E	
%06	Ctrl-F	
%07	Ctrl-G	aka Bell
%08	Ctrl-H	aka Backspace
%09	Ctrl-I	aka Tab
%0A	Ctrl-J	aka Line Feed or Newline
%0B	Ctrl-K	
%0C	Ctrl-L	aka Form Feed or Redraw Screen
%0D	Ctrl-M	aka Enter
%0E	Ctrl-N	
%0F	Ctrl-O	
%10	Ctrl-P	
%11	Ctrl-Q	
%12	Ctrl-R	
%13	Ctrl-S	
%14	Ctrl-T	
%15	Ctrl-U	
%16	Ctrl-V	
%17	Ctrl-W	
%18	Ctrl-X	
%19	Ctrl-Y	
%1A	Ctrl-Z	Sometimes used as EOF or suspend signal
%1B	Escape	
%25	Percent	The actual % character
%7F	Delete	

Translating Table Statements

This is the byte-mapping table definition. Any number of mapping tables can be defined, as long as each one has a unique table name. Usually a different table is used for inbound (to host) and outbound (from host) translation.

Use the following format to enter a table statement entry in the TermProxy configuration:

```
table [table name]
<source byte 1>=<destination byte 1>
<source byte 3>=<destination byte 3>
<source byte n>=<destination byte n>
```

Table 3-5 contains detailed information about the table statement entry.

Parameter	Description
table name	This is a freely chosen name for the table. The hostservice translate-fromhost and translate-tohost keywords refer to the table using this name.
source byte=destination byte	The byte mapping instructions immediately follow the table keyword and must be codes as shown. Do not use spaces around the '='. The source and destination byte can either be an ASCII character or an escaped-byte value.

Table 3-5: *TermProxy Table Statement Parameters*

The following are some mapping examples:

```
Table Table1

%00=?  //Replaces a NUL with a question mark
==%20  //Replaces an equal sign with an ASCII blank
1=%f1  //Replaces an ASCII 1 with an EBCDIC 1
```

Validating Configuration Entries

Once you have entered the TermProxy configurations, you can validate your entries to ensure accuracy.

To validate configuration entries:

1. Complete TermProxy configurations.
2. Click the `Validate` button at the bottom of the *TermProxy Configuration* page.

If an entry contains invalid configurations, an error message appears at the bottom of the window stating which part of the configuration contains errors.

Saving and Restarting Configurations

TermProxy configurations must be saved and the application restarted for configuration modifications to take effect.

To save and restart:

1. Click the `Save and Restart` button at the bottom of the *TermProxy Configuration* window.

   The system takes a moment to restart, and then the *TermProxy Main Menu* page appears.

2. Return to the *TermProxy Configuration* page to ensure your changes were saved.

Sample Configurations

The following section contains two sample TermProxy configurations and detailed descriptions of each parameter in the sample configurations.

Sample Configuration 1

```
proxyservice TelnetOne
listen 0.0.0.0:2301
server TelnetHost
timeout 5
ssl on

hostservice TelnetHost
connect 192.168.1.1:23
timeout 60
reconnect-string %0c
undeliverable ABORT
codeset ASCII
```

The following table provides a detailed description of each parameter in Sample Configuration 1.

Sample TermProxy Configuration 1	Parameter Description
`proxyservice TelnetOne`	The proxyservice name is TelnetOne.
`listen 0.0.0.0:2301`	The proxyservice listens for mobile devices on any local IP interface with 2301 as the listen port.
`server TelnetHost`	The proxyservice services the hostservice named TelnetHost.
`timeout 5`	The client-proxy connection will time out after five minutes of inactivity.
`ssl on`	mobile devices must use SSL to access a hostservice using the TelnetOne proxyservice.
`hostservice`	The hostserivce name is TelnetHost. TelnetHost is referenced within the proxyservice TelnetOne.
`connect 192.168.1.1:23`	When a mobile device connects to the proxyservice “TelnetOne” using the a host profile that contains 192.168.1.1:23, the TermProxy establishes a connection with the target host 192.168.1.1:23.
`timeout 1h`	Once the client-proxy connection closes (see proxyservice timeout), the proxy-host connection closes after one hour of inactivity.
`reconnect-string %0c`	The reconnect entry instructs the mobile device to send the command `%0c` to the host upon reconnect.
`undeliverable ABORT`	If the host sends an unsolicited message while the mobile device is unavailable, both the client-proxy and the proxy-host connection will be dropped.
`codeset ASCII`	The capture data displays in ASCII.

Table 3-6: *Sample Configuration 1 Parameter Descriptions*

Sample Configuration 2

```
proxyservice "TelnetHosts"
  listen 20.30.40.50:4430
  server "Host AS400”, “Host VT"

hostservice "Host AS400"
  connect 206.125.145.25:23
  reconnect-string
  %00%0D%12%A0%00%00%04%00%00%03%01%01%33%FF%EF
  codeset EBCDIC
  stationid-template “Display [.] +:\s+ (.t?) []”
```

```
hostservice "Host VT"
  connect 207.95.165.10:23

loglevel info

httpservice 127.0.0.1:6666
  ssl on
```

The following table provides a detailed description of each parameter in Sample Configuration 2.

Sample TermProxy Configuration 2	Description
`proxyservice TelnetHosts`	The proxyservice name is TelnetHosts.
`listen 20.30.40.50:4430`	The proxyservice listens for mobile devices at 20.30.40.50 and port 4430.
`server "Host AS400", "Host VT"`	The proxyservice services two hostservices named "Host AS400" and "Host VT".
	Timeout and SSL parameters are not specifically defined in this sample configuration. These parameters default to timeout 24 hours and SSL Off.
`hostservice "Host AS400"`	The first hostservice name is "Host AS400".
`connect 206.125.145.25:23`	When a mobile device connects to the proxyservice "TelnetHosts" using the a host profile that contains 206.125.145.25:23, the TermProxy establishes a connection with the target host 206.125.145.25:23.
`reconnect %00%0D%12%A0%00%00%04%00%00%03%01%01%33%FF%EF`	This reconnect string sends an `F3` upon reconnect.
`codeset EBCDIC`	The EBCDIC codeset allows the workstation ID to display in the Session List page of the TermProxy web interface.
`stationid-template "Display [ .] +:\s+(.t?) [ ]"`	The stationid-template allows the workstation ID to display in the *Session List* page of the TermProxy web interface.
`hostservice "Host VT"`	The second hostservice name is "Host VT".
`connect 207.95.165.10:23`	When a mobile device connects to the proxyservice "TelnetHosts" using the a host profile that contains 207.95.165.10:23, the TermProxy establishes a connection with the target host 207.95.165.10:23.
`log level INFO`	The log level entry instructs the proxy server to log information at the INFO level only.

Table 3-7: *Sample Configuration 2 Parameter Descriptions*

Sample TermProxy Configuration 2	Description
`httpservice 201.120.140.10:4428`	The httpservice entry instructs the proxy server to bind the HTTP server to the IP address 201.120.140.10 on port 4428.
`ssl on`	The ssl entry instructs the proxy server to use the SSL protocol.

Table 3-7: *Sample Configuration 2 Parameter Descriptions*

Chapter 4: Using TermProxy

This chapter provides information about using TermProxy, including:

- TermProxy Functionality
- Using TermProxy with Telnet Client
- TermProxy Web Interface Operations
- Logging and Data Capture
- TermProxy HTTP settings
- Viewing TermProxy Status and Sessions
- Running TermProxy as a Service

TermProxy Functionality

The connection between the mobile device and TermProxy is referred to as the client-proxy connection (Figure 4-1 P1 and P2). The connection between TermProxy and the host is referred to as the proxy-host connection (Figure 4-1 P1 and P2). The TermProxy base functionality utilizes the following two internal modules:

- **Proxyservice.** The proxyservice module listens for mobile device requests on the port number defined in the proxyservice entry within the TermProxy configuration file. TermProxy takes these requests and makes a logical connection to one of the hostservices it accommodates.
- **Hostservice.** The hostservice module establishes a connection with the Telnet server process on the target host.

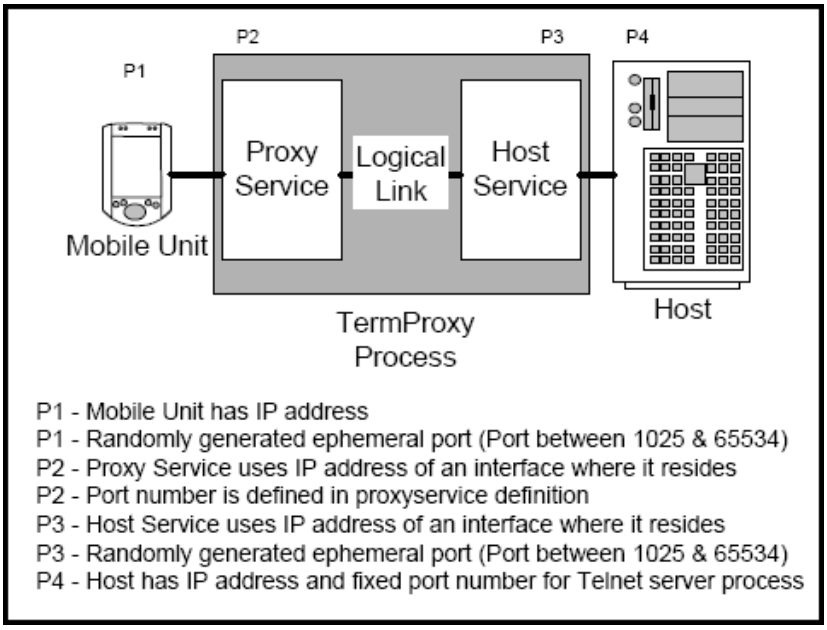

Figure 4-1. *Process Overview*

The TermProxy process may reside on the same machine as the Telnet server. Typically the OS/400 deployment of TermProxy will reside on the same system as the Telnet server.

Each mobile device session is identified by a unique session ID when the Telnet session is established through TermProxy. This allows multiple Telnet sessions on one mobile device to be established through TermProxy.

Using TermProxy with Telnet Client

This section describes the basic steps for initiating a Telnet session with TermProxy. It also provides more detailed instructions about configuring the host profile, including the host and TermProxy profiles. The following information is included:

- Initiating a Telnet Session with TermProxy
- Configuring the Telnet Host Profile
- SSL/TLS Encryption and Verification

- SSH Encryption and Verification
- Custom Encryption

Initiating a Telnet Session with TermProxy

Use the following steps to establish a Telnet Session with TermProxy.

To initiate a Telnet session with TermProxy:

1. Install TermProxy.
2. Add proxyservice and hostservice configurations using the TermProxy web interface.
3. Add a host profile with TermProxy from the Telnet configuration utility.
4. Connect to the Telnet host using TermProxy.

NOTE If you are using a firewall, make sure you have properly configured your static NAT tables and access lists.

---

5. View the status of your connection from the TermProxy web interface to verify TermProxy is being used for the Telnet session.

Configuring the Telnet Host Profile

You need to configure both the Host tab and the TermProxy 1 tab in the *Host Profiles* dialog box of the Telnet configuration utility.

Host tab

Configure the Host tab of the Host Profile before configuring the TermProxy 1 tab.

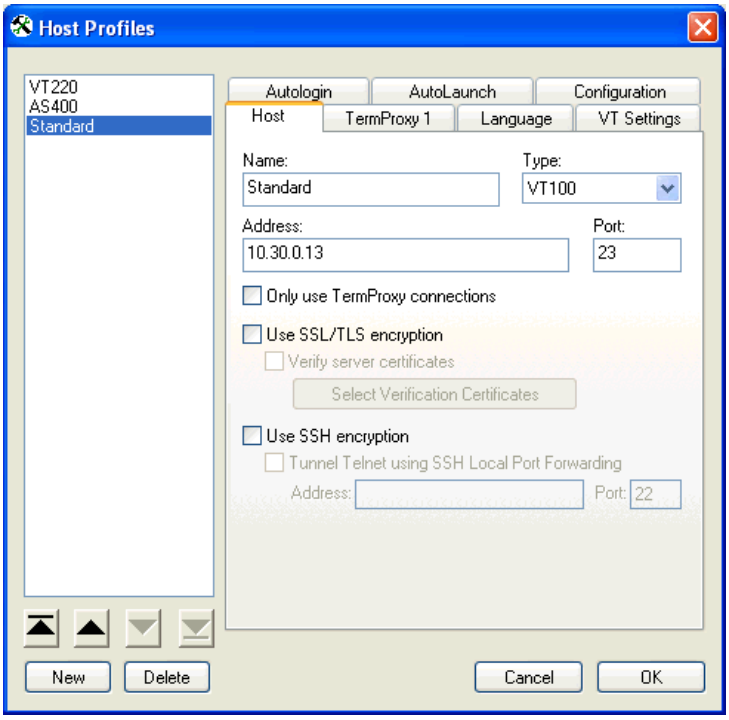

Figure 4-2. *Host Profiles Dialog Box*

The following table describes the configuration options for the Host tab.

Configuration Option	Description
Name	Enter the name of the Telnet host profile. This field is required.
Type	Select the type of emulation. This field is required.
Address	Enter the IP address of the Telnet host. This field is required.
Port	Enter the port of the Telnet host. This field is required.

Table 4-1: *Host Tab Configuration Options*

Configuration Option	Description
Only use TermProxy connections	Enable this option if you want to use TermProxy connections only. This prevents direct connections to the target host. This option disables the **Use SSL/TLS encryption** option for the Telnet host, but not for TermProxy. This feature is optional.
Use SSL/TLS encryption	Enable this option if you want to use SSL/TLS to encrypt the data between the mobile device and the Telnet Host. If you enable this option, the **Only use TermProxy connections** option will disable. This feature is optional.
Verify server certificates	Enable this option if you want to use verification certificates. The **Use SSL/TLS encryption** must be enabled for this option to be active. Clients use certificates to verify that they are communicating with the correct server. SSL/TLS verification requires a local certificate chain (root certificate and intermediate certificates if any) on the mobile device. This feature is optional.
Select Verification Certificates	This allows you to create verification certificates. Refer to *SSL/TLS Encryption and Verification* on page 56 for more information. The **Verify server certificates** option must be enabled for this option to be active. This feature is optional.
Use SSH encryption	Enable this option if you want to use SSH to encrypt the data between TermProxy and the host. If you enable this option, the **Only use TermProxy connections** option will disable. This feature is optional.
Address	Enter the IP address of the SSH host. This feature is optional.
Port	Enter the port of the SSH host. This feature is optional.

Table 4-1: *Host Tab Configuration Options*

TermProxy 1 Tab

Once you configure the Host tab, you need to configure the TermProxy 1 tab.

You can configure up to three TermProxy servers as failover servers. If the initial TermProxy server cannot be reached, it attempts to connect to all

available subsequent TermProxy servers before it attempts a direct connection with the Telnet host. Options to configure the TermProxy 2 tab become available after you configure the TermProxy 1 tab. Options to configure the TermProxy 3 tab become available after you configure the TermProxy 2 tab.

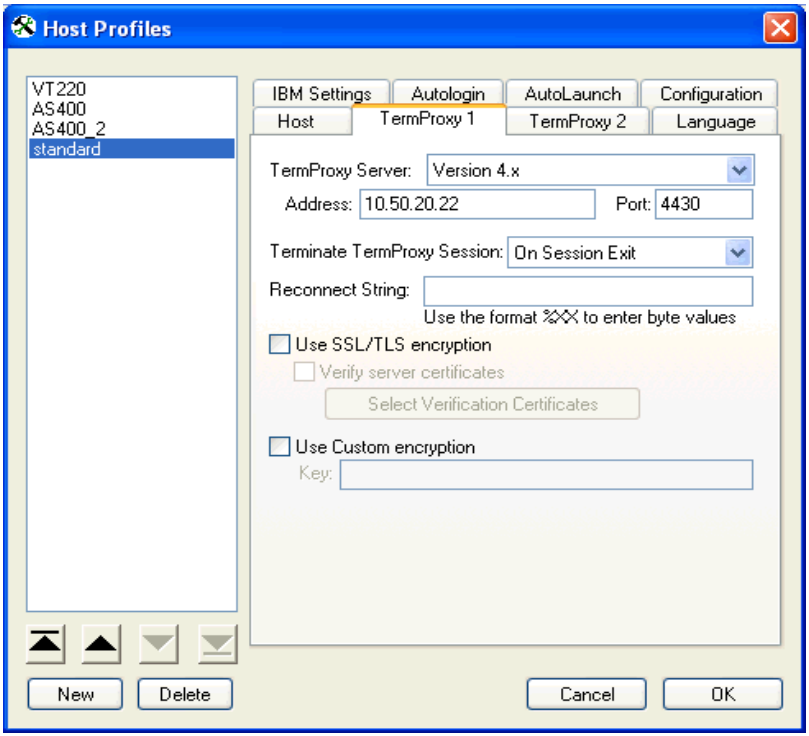

Figure 4-3. *TermProxy 1 Tab*

The following table describes the configuration options for the TermProxy 1 tab.

Configuration Option	Description
TermProxy Server	Select the version of TermProxy you want to run. This field is required.
Address	Enter the IP address of the TermProxy server. This field is required.

Table 4-2: *TermProxy Configuration Options*

Configuration Option	Description
Port	Enter the Port of the TermProxy server. This field is required.
Terminate TermProxy Session	You can select the method by which TermProxy handles session disconnects. **On Session Exit**. When the you close the Telnet session intentionally using `Alt-T` from the external keyboard or `Disconnect Session` from the Telnet Client menu, both client-proxy and proxy-host connections close. This is the default option and recommended in most cases. **Always**. When you close the Telnet session intentionally using `Alt-T` from the external keyboard or `Disconnect Session` from the Telnet Client menu, both client-proxy and proxy-host connections close. Client-proxy and proxy-host connection also close when the mobile device is warm-booted or the client-proxy connection is lost (I.e., powered off, went to sleep for an extended period of time, etc.). **Never**. When you close the Telnet session intentionally using `Alt-T` from the external keyboard or `Disconnect Session` from the Telnet Client menu, the proxy-host connection remains open. The client-proxy and proxy-host connections also remain open when the mobile device is warm-booted or the client-proxy connection is lost (I.e., powered off, went to sleep for an extended period of time, etc.). **On Network error**. The Telnet session will disconnect only when a network error occurs. Default: **On Session Exit**

Table 4-2: *TermProxy Configuration Options*

Configuration Option	Description
Reconnect String	Input a reconnect string or use one you defined in the TermProxy configuration file. When a mobile device unintentionally disconnects from TermProxy, the proxy-host connection remains active until a mobile device reconnects or the hostservice time-out is reached. A reconnect-string is required in 5250 and 3270 environments. Reconnect-string requirements depend upon the application. The purpose of the reconnect-string is to request the last screen data that the host had before the mobile device disconnected. There may be cases where the screen data that the host has does not reflect the screen data that was present on the device before the disconnect. In these cases, you will need to send a reconnect-string that will place the user at a desired point in the application. For example, if you are in a VT application and the client-proxy connection was unintentionally disconnected, the host may only have a portion of the actual screen. This is because the host may have required multiple conversations to paint the screen that existed on the mobile device before the client-proxy disconnect. Therefore, you need to pick a reconnect string such as a function key, escape sequence, or the `Enter` key that will cause your application to repaint the desired transaction screen or menu. The reconnect string in the host profile takes precedence over the reconnect string configured in the TermProxy configuration file. A reconnect-string is required in 5250 and 3270 environments.

Table 4-2: *TermProxy Configuration Options*

Configuration Option	Description
Use SSL/TLS encryption	Enable **Use SSL/TLS encryption** to encrypt data between the mobile device and the TermProxy server. You can enable the **Use SSL/TLS encryption** option to encrypt the data between the mobile device and the TermProxy server. **NOTE** SSL/TLS communication is not an option between the TermProxy server and the target Telnet host due to the additional processing it would require. Also, it is presumed that the TermProxy-to-Host communications will take place on the trusted network. Refer to *SSL/TLS Encryption and Verification* on page 56 for more information. This feature is optional.
Verify server certificates	Enable **Verify Server Certificates** to perform SSL/TLS verification between the mobile device and the TermProxy server. SSL/TLS verification requires a local certificate chain (root certificate and intermediate certificates if any) on the mobile device. Refer to *SSL/TLS Encryption and Verification* on page 56 for more information. This feature is optional.
Select Verification Certificates	Once you enable the **Verify Server Certificates** option, the `Select Verification Certificates` button is active. Click this button to open the *Certificate Manager* dialog box. You can use the Certificate Manager to create, insert or remove certificates. Refer to *SSL/TLS Encryption and Verification* on page 56 for more information. This feature is optional.
Use Custom encryption	Enable **the Use Custom encryption** option to encrypt data between the mobile device and the TermProxy server. This feature is optional.
Key	Once you enable the **Use Custom encryption** option, the **Key** text box is active. Type the password specified in the TermProxy configuration in the text box.

Table 4-2: *TermProxy Configuration Options*

SSL/TLS Encryption and Verification

You need to install the SSL/TLS support utility on the PC, then deploy another SSL/TLS support utility to the mobile device. Once you have installed the support utility you can enable SSL/TLS encryption and certificates. This section provides the following information:

- Installing the SSL/TLS Support Utility on the PC
- Deploying the SSL/TLS Support Utility to the Mobile Device
- Enabling SSL/TLS Support
- Enabling SSL/TLS Verification
- Creating a New Certificate
- Inserting Verification Certificates
- Removing a Certificate

NOTE Contact Wavelink Customer Service for information on obtaining the SSL/TLS support utility. Refer to *Appendix C: Wavelink Contact Information* on page 97 for more information.

Installing the SSL/TLS Support Utility on the PC

Install the Windows SSL/TLS support utility on the PC from which you deploy the Telnet Client.

To install the SSL/TLS support utility on the PC:

1. Obtain the installation executable for the Windows SSL/TLS support utility.
2. Install the SSL/TLS support utility on the PC from which you deploy the Telnet Client.

Deploying the SSL/TLS Support Utility to the Mobile Device

You can use Avalanche or ActiveSync to deploy the SSL/TLS support utility to the device.

To deploy the SSL/TLS utility through Avalanche:

1 Obtain the Avalanche SSL/TLS support file.

NOTE If you do not know the processor type of your mobile device (ARM or X86), install both the ARM and X86 SSL/TLS support packages. Avalanche selection criteria will ensure that the correct SSL/TLS support package is downloaded to the mobile device based upon the package selection criteria.

---

2 From the **Software Management** menu in Avalanche Management Console, select `Install Software Package`.

3 Browse to the location of the Avalanche SSL/TLS support package and select the package.

4 Select the software collection where you want to install the SSL/TLS support package.

5 Click `Next`.

The *License Agreement* dialog box appears.

6 Click `Yes` to accept to the license agreement.

7 Enable the SSL/TLS support package.

8 Perform an Avalanche update on the device to download the SSL/TLS support package to the device.

To deploy the SSL/TLS utility using ActiveSync:

1 Obtain the SSL/TLS ActiveSync executable.

2 Create a Microsoft ActiveSync connection between the host PC and the mobile device. (You may use either a Guest Partnership or a Standard Partnership.)

3 On the host PC, launch the SSL/TLS ActiveSync executable to deploy the executable to the mobile device.

4 Launch the Telnet Client.

Enabling SSL/TLS Support

The SSL/TLS support is configured from the *Host Profiles* dialog box of the Telnet configuration utility.

NOTE SSL/TLS is only an active option if SSL/TLS support has been installed on the PC running the Telnet Client configuration utility.

To configure SSL/TLS:

1. Access the host profiles configuration utility for the Telnet Client.
2. Select or create a new host profile.
3. Add a TermProxy server in the TermProxy 1 tab.
4. Enable the **Use SSL/TLS encryption** option in the TermProxy 1 tab.
5. Click `OK`.
6. Deploy the new Telnet Client configuration to the mobile device.

Enabling SSL/TLS Verification

Use the TermProxy 1 tab in the *Host Profiles* dialog box to enable certificates. Once you enable the certificates, you have the option to create, insert, or remove certificates.

To enable certificates:

1. Access the host profiles configuration utility for the Telnet Client.
2. In the TermProxy 1 tab, within the *Host Profiles* dialog box, enable the **Verify server certificates** option.

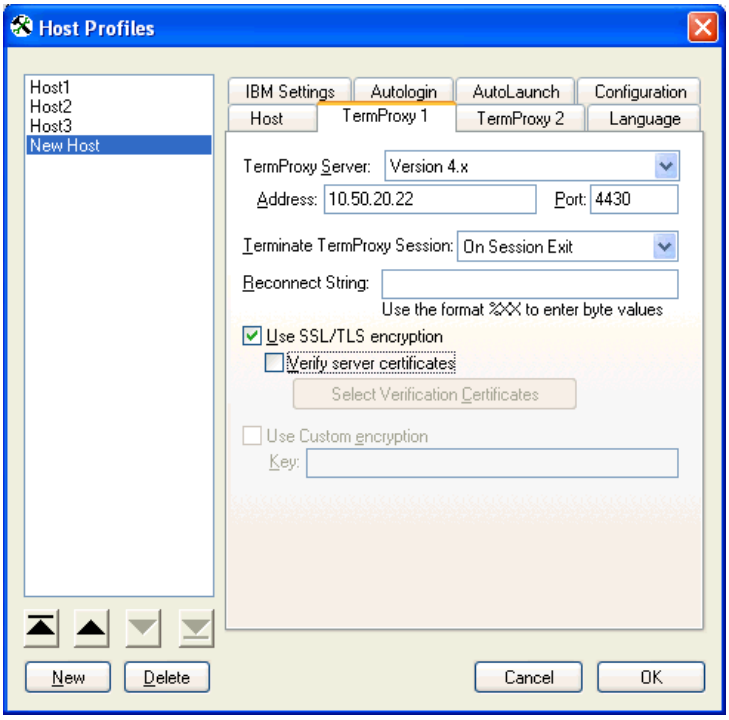

Figure 4-4. *Enabling Certificates*

3 Click the `Select Verification Certificates` button.

The *Certificate Manager* dialog box appears.

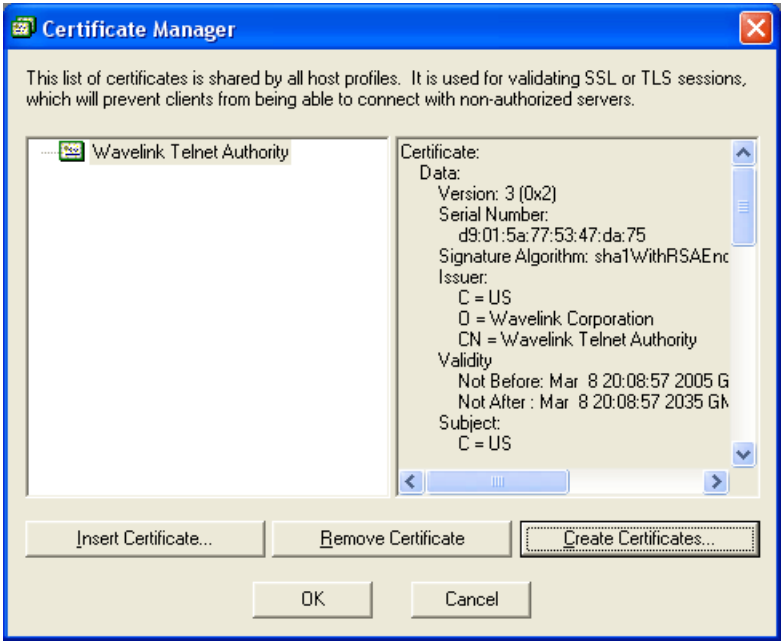

Figure 4-5. *Certificate Manager Dialog Box*

4 Use the *Certificate Manager* dialog box to create, insert, or remove a certificate for use with TermProxy.

Creating a New Certificate

The `Create Certificates` button in the *Certificate Manager* dialog box generates a certificate that can be used to verify that a Telnet Client is communicating with the correct TermProxy or Telnet server. You have the option to copy the server certificate to the TermProxy installation folder. (For Win32, copy the certificates to the folder where `WLTermProxyService.exe` resides. The default Win32 installation folder is `c:\Program Files\Wavelink\TermProxy`. For OS/400, copy the certificates to `/home/wtermproxy`.)

NOTE TermProxy should be installed before you create certificates.

To create a new certificate:

1 Access the *Certificate Manager* dialog box.

2 Click the `Create Certificates` button.

The *Create Certificates* dialog box appears.

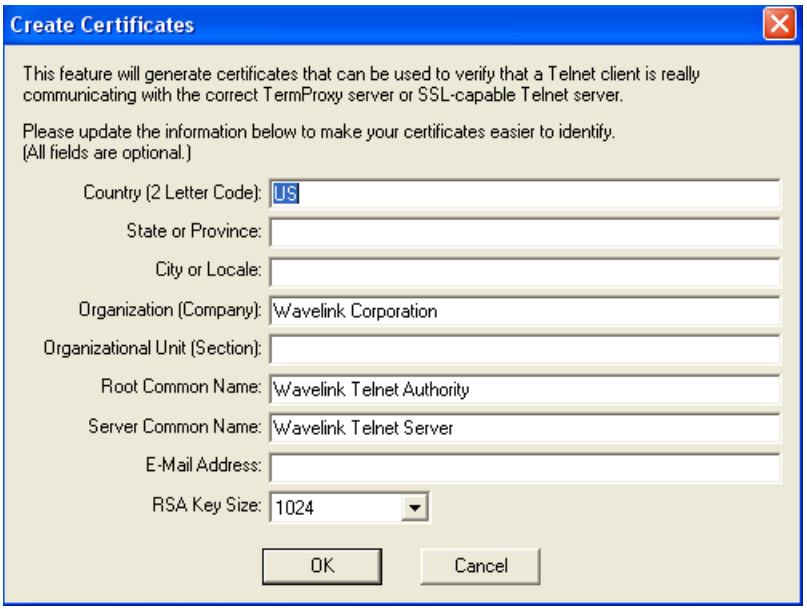

Figure 4-6. *Create Certificates Dialog Box*

3 Enter the certificate information.

4 Click `OK`.

5 For Win32, follow the prompts to copy `servercert.pem` and `serverkey.pem` files to the Win32 TermProxy installation directory.

6 For AS/400, manually copy the `servercert.pem` and `serverkey.pem` files to `/home/wtermproxy`.

7 Save the host profile and deploy the configuration to the mobile device.

Inserting Verification Certificates

To use your own certificate authority with TermProxy, you need to convert your server certificate and private key to PEM format. Once converted, you need to copy the `servercert.pem` and `serverkey.pem` files to the location where the TermProxy configuration files are installed.

To insert a certificate:

1 Access the *Certificate Manager* dialog box.

2 Convert your server certificate and server key to PEM format.

3 Click the `Insert Certificate` button.

4 Browse to the certificate file.

5 Click `Open`.

6 For Win32, follow the prompts to copy `servercert.pem` and `serverkey.pem` files to the Win32 TermProxy installation directory. The default location is `c:\Program Files\Wavelink\TermProxy`.

7 For AS/400, manually copy the `servercert.pem` and `serverkey.pem` files to `/home/wtermproxy`.

8 Save the host profile and deploy the configuration to the mobile device.

Removing a Certificate

You can remove a certificate if you no longer want to use it.

To remove a certificate:

1 Access the *Certificate Manager* dialog box.

2 Select the certificate you want to remove.

3 Click the `Remove Certificate` button.

SSH Encryption and Verification

Use the **Host** tab in the host profiles configuration utility to configure SSH encryption.

To configure SSH:

1 Access the host profiles configuration utility for the Telnet Client.

2 Select or create a new host profile.

3 Enable the **Use SSH encryption** checkbox and enter the IP address and port in the appropriate text boxes.

4 Click `OK`.

The host profile configuration utility closes and your changes are saved.

Custom Encryption

The **Use Custom encryption** option allows you to enter a password (or encryption key) to encrypt information between the TermProxy server and mobile devices that cannot support SSL encryption.

To configure custom encryption:

1. Access the host profiles configuration utility for the Telnet Client.
2. Select or create a new host profile.
3. Add a TermProxy server in the TermProxy 1 tab.
4. Enable the **Use Custom encryption** checkbox and enter the encryption key in the **Key** text box.

NOTE The encryption key must match the key specified in the TermProxy configuration.

---

5. Click `OK`.

   The host profiles configuration utility closes and your changes are saved.

TermProxy Web Interface Operations

This section provides information about the following TermProxy web interface options:

- Accessing the TermProxy Web Interface
- Viewing the TermProxy Readme File
- Viewing the TermProxy Release Notes
- Restarting TermProxy

Accessing the TermProxy Web Interface

You need to know the IP address and port of the TermProxy HTTP server and the user name and password to access the TermProxy web interface.

To access the TermProxy web interface:

1 Launch a web browser.

2 In the address field of the web browser, type the address and port of the TermProxy HTTP server using the following format:

`http://[ipaddr]:[port]`

where

- `[ipaddr]` is the IP address of the TermProxy web server
- `[port]` is the TCP port of the TermProxy web server

3 Enter the user name and password.

The *TermProxy Main Menu* page appears.

Viewing the TermProxy Readme File

You can view the TermProxy readme file from the TermProxy web interface.

To view the TermProxy readme file:

1 Access the TermProxy web interface.

2 From the *TermProxy Main Menu* page, click `Configuration`.

The *Logging and Data Capture Settings* window appears.

3 In the left-channel navigation, click `View README`.

The readme file appears in a separate web browser.

Viewing the TermProxy Release Notes

You can view the TermProxy release notes from the TermProxy web interface.

To view the TermProxy release notes:

1 Access the TermProxy web interface.

2 From the *TermProxy Main Menu* page, click `Configuration`.

The *Logging and Data Capture Settings* page appears.

3 In the left-channel navigation, click `View Release Notes`.

The release notes open in a separate web browser.

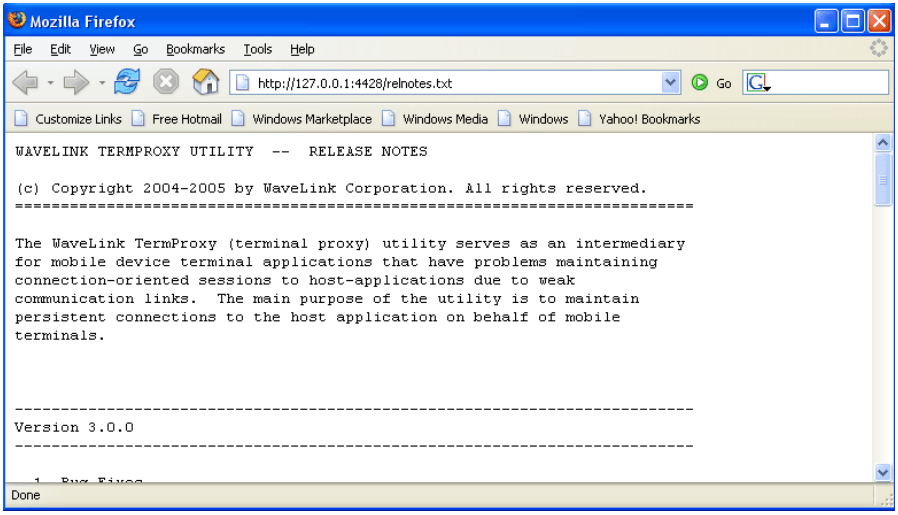

Figure 4-7. *Release Notes*

Restarting TermProxy

You can restart TermProxy from the *Restart TermProxy* page in the TermProxy web interface or from the TermProxy configuration.

To restart TermProxy from the *Restart TermProxy* page:

1 Access the TermProxy web interface.

2 From the *TermProxy Main Menu* page, click `Configuration`.

The *Logging and Data Capture Settings* page appears.

3 In the left-channel navigation, click `Restart TermProxy`.

The *Restart TermProxy* page appears.

4 Click the `Restart` button.

NOTE It may take up a minute to restart TermProxy. Once TermProxy is restarted, the TermProxy *Main Menu* page appears. If the TermProxy *Main Menu* page does not open after one minute, refresh the browser connection.

To restart TermProxy from the TermProxy configuration:

1 Access the TermProxy web interface.

2 From the *TermProxy Main Menu* page, click `Configuration`.

The *Logging and Data Capture Settings* page appears.

3 In the left-channel navigation, click `Proxy Configuration`.

The *TermProxy Configuration* page appears.

4 In the TermProxy configuration, type `restart [time]`, where `[time]` is a comma-delimited list of times that TermProxy will automatically restart. Enter times using the following format: `HH:MM [a|p]`. If there is no `a` (A.M.) or `p` (P.M.) indicated, the time is assumed to be in 24-hour format. Specify a weekly time by preceding the time with the day of the week.

Example:
```
10:00P
MONDAY22:30
```

5 Click `Save and Restart` to apply the new settings.

Logging and Data Capture

This section provides information about TermProxy logging and data capture, including the following:

- Overview
- Setting the Logging Level
- Enabling Data Capture

- Viewing Files
- Refreshing Files

Overview

TermProxy provides a logging service that writes information about TermProxy functions to a plain-text log file. This information allows you to evaluate errors, TermProxy server functionality, and information about client connection.

The amount of detail that is recorded to the TermProxy log file is user-configurable. TermProxy allows you to specify the logging level, which determines the types of information recorded to the log file. For more information on logging levels, see *TermProxy Logging Levels* on page 67.

The log file is called `TermProxy.log` and is generated in the directory from which you are running the TermProxy application.

Whenever TermProxy starts, it creates a new `TermProxy.log` file. Before this occurs, however, TermProxy writes the contents of the previous `TermProxy.log` to the `TermProxy.log.bak` file.

While TermProxy is running, TermProxy will not allow the log file to grow beyond 100 KB. Once the log file reaches 100 KB, TermProxy creates a new log file called `TermProxy.log.xxx`, where `xxx` is a sequential number that begins at 001. The contents of these additional log files are also written to `TermProxy.log.bak`, when TermProxy is started.

TermProxy Logging Levels

TermProxy provides six logging levels. The following table describes the type of information that will be written to `TermProxy.log` for each level.

Log Level	Information Written to TermProxy.log
Level 1	Writes only critical errors to the log file.
Level 2	Writes critical errors and error messages to the log file.
Level 3	Writes critical errors, error messages, and warnings to the log file.
Level 4	Writes critical errors, error messages, warnings, and informational messages to the log file.

Table 4-3: *TermProxy Logging Levels*

Log Level	Information Written to TermProxy.log
Level 5	Writes critical errors, error messages, warnings, informational messages, and debug information to the log file.
Level 6	Writes critical errors, error messages, warnings, information messages, debug information and all other information to the log file.

Table 4-3: *TermProxy Logging Levels*

The following list provides a description of the type of messages that may be written to the log file:

Critical Indicates errors that cause TermProxy to fail to start.

Error Indicates errors that are caused by configuration and/or communication problems.

Warning Indicates possible operational problems.

Informational Documents the flow of operation.

Debug Used to diagnose program malfunctions or communication problems.

Verbose Indicates and documents all errors, operational problems, program malfunctions or communication problems. (This logging level causes large amounts of data to be written to the log file.)

Setting the Logging Level

By default, TermProxy is set to logging level 4. You can modify the TermProxy logging level in the TermProxy web interface two ways:

- In the TermProxy configuration
- In the *Logging and Data Capture Settings* page

To modify the logging level in the TermProxy configuration:

1. Access the TermProxy web interface.
2. From the *TermProxy Main Menu* page, click `Configuration`.

   The *Logging and Data Capture Settings* page appears.
3. In the left-channel navigation, click `Proxy Configuration`.

4 In the configuration text box, type `loglevel [level]`, where `[level]` is the logging level you want to set.

Example: `loglevel debug`

5 Click `Validate` to validate your changes.

6 Click `Save and Restart` to save your changes and restart TermProxy.

To modify the logging level from the *Logging and Data Capture Settings* page:

1 Access the TermProxy web interface.

2 From the *TermProxy Main Menu* page, click `Configuration`.

The *Logging and Data Capture Settings* page appears.

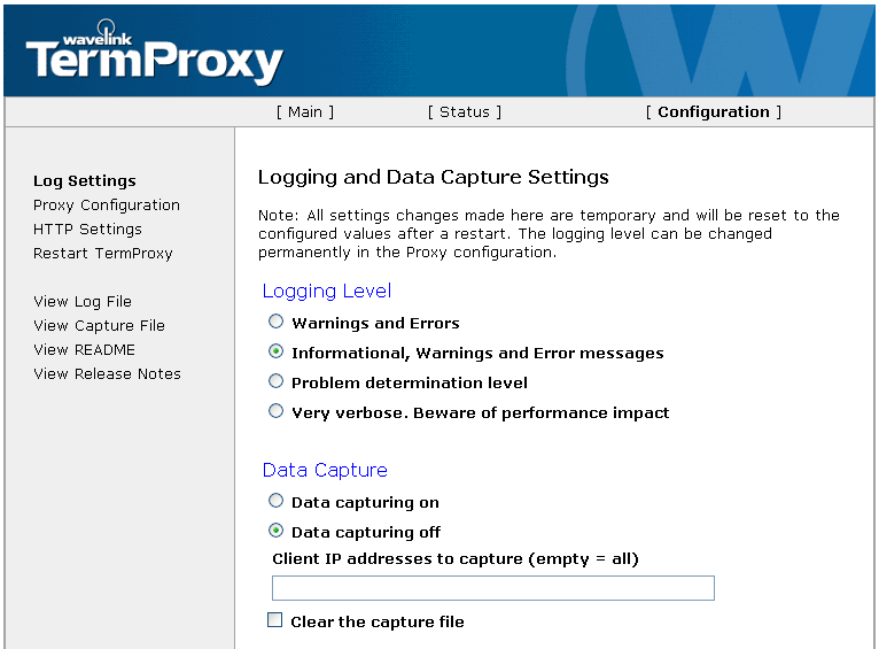

Figure 4-8. *Logging Levels*

3 Select the logging level.

4 Click `Apply Changes`.

NOTE All changes made in the *Logging and Data Capture Settings* page are temporary and will reset to the configured values after a restart. To ensure logging levels remain permanent, set the level in the *TermProxy Configuration* page.

Enabling Data Capture

Data capture records all network traffic entering and exiting the TermProxy program.You can enable data capturing from the *Logging and Data Capture Settings* page or in the TermProxy configuration. By default the data capturing mode is set to off. The data capturing function is a temporary setting and needs to be enabled after each TermProxy restart to continue capturing data.

To enable data capturing from the TermProxy configuration:

1. Access the TermProxy web interface.
2. From the *TermProxy Main Menu page*, click `Configuration`.

   The *Logging and Data Capture* page appears.
3. In the left-channel navigation, click `Proxy Configuration`.
4. In the configuration text box, type `capture [status]`, where `[status]` and `clear [status]`, where `[status]` is the preferred setting (on or off).

   Example:
   ```
   capture on
   clear off
   ```
5. Click `Validate` to validate your changes.
6. Click `Save and Restart` to save your changes and restart TermProxy.

To enable data capturing from the *Logging and Data Capture Settings* page:

1. Access the TermProxy web interface.
2. From the *TermProxy Main Menu* page, click `Configuration`.

   The *Logging and Data Capture Settings* page appears.
3. Enable the **Data capturing on** option to enable data capture mode.

4 In the **Client IP addresses to capture** text box, enter the IP addresse(s) of the clients from which you want to capture data.

NOTE You can restrict the data capture to an individual IP address, multiple IP addresses comma delimited, or a network.

Examples:

Individual: [`165.138.5.10`]

Multiple: [`165.192.5.10, 10.204.140.50`]

Network: [`165.192.5.1/24`]

NOTE If you leave the **Enter IP addresses to capture** text box empty, all client data will be captured.

---

5 Click `Apply Changes`.

NOTE All changes made in the *Logging and Data Capture Settings* page are temporary and will be reset to the configured values after a restart.

Viewing Files

You can view the TermProxy log file and data capture file from the web interface.

To view a TermProxy log file:

1 Access the TermProxy web interface.

2 From the *TermProxy Main Menu* page, click `Configuration`.

The *Logging and Data Capture Settings* page appears.

3 In the left-channel navigation, click `View Log Files`.

The log file appears in a separate window.

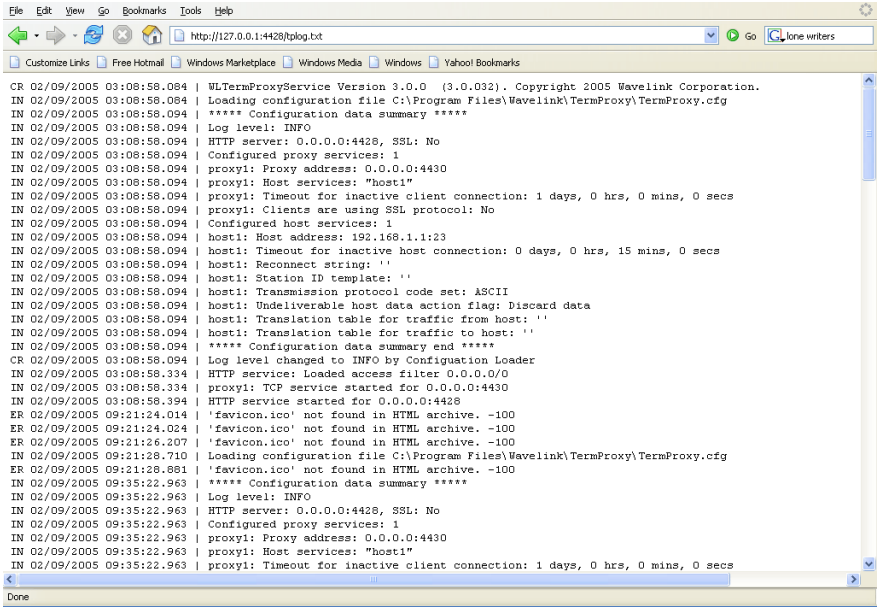

Figure 4-9. *Log File*

To view the data capture file:

1 Access the TermProxy web interface.

2 From the *TermProxy Main Menu* page, click `Configuration`.

The *Logging and Data Capture Settings* page appears.

3 In the left channel navigation, click `View Capture File`.

The data capture file appears in a separate window.

NOTE If the **Data capturing on** option is not enabled, there will be no information written to the data capture file.

Refreshing Files

Once you have a log file or data capture browser page open, the page remains open. You can refresh the page to view the most current activity written to the log.

To refresh the TermProxy log file:

- Browse to the open TermProxy log file page and click the `Refresh` button at the top of the page.

-Or-

- In the *Logging and Data Capture Settings* page, click `View Log File` and browse to the open TermProxy log file page.

To refresh the TermProxy data capture:

- Browse to the open TermProxy data capture page and click the `Refresh` button at the top of the page.

-Or-

- In the *Logging and Data Capture Settings* page, click `View Data Capture` and browse to the open data capture page.

TermProxy HTTP settings

This section provides information on TermProxy HTTP settings including the following:

- Overview of TermProxy HTTP settings
- Changing TermProxy HTTP Settings

Overview of TermProxy HTTP settings

The TermProxy *HTTP Settings Page* allows you to manage TermProxy web server access. You can use the *HTTP Settings Page* to perform the following tasks:

- Change the username and password for the TermProxy web server
- Restrict access to an individual IP node, multiple IP nodes, or to a network
- Configure encryption for the administration file (http.cfg)

Both the Win32 and the AS/400 installation programs allow you to make HTTP setting changes that will persist when TermProxy is restarted. The

HTTP settings are saved to the `http.cfg` file for both Win 32 and AS/400 products.

Changing TermProxy HTTP Settings

You need the administrative password to make changes to the TermProxy HTTP settings. The administrative password is different from the browser password you needed to start the session.

To change HTTP settings:

1 Access the TermProxy web interface.

2 From the *TermProxy Main Menu* page, click `Configuration`.

The *Logging and Data Capture Settings* page appears.

3 In the left-channel navigation, click `HTTP Settings`.

The *HTTP Settings* page appears.

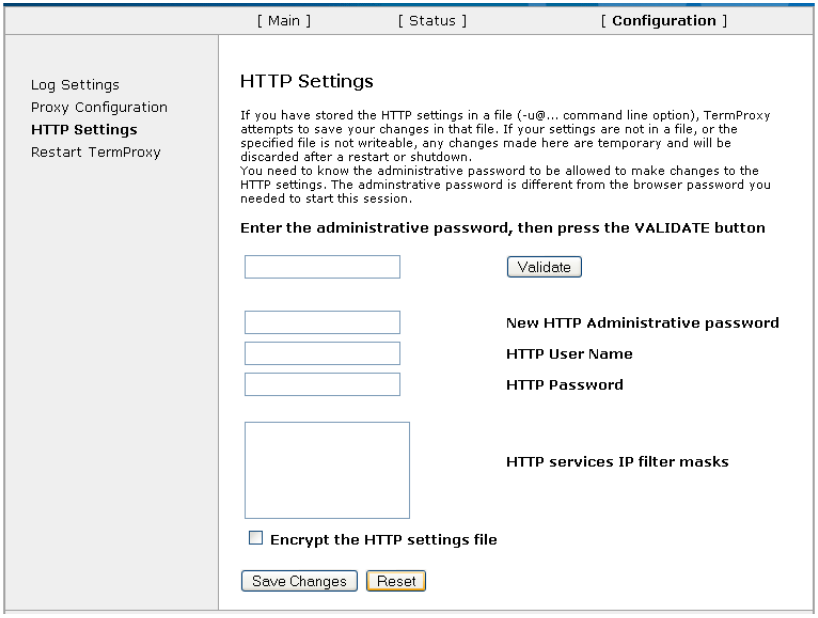

Figure 4-10. *HTTP Settings*

4 Enter the administrative password and click `Validate`.

NOTE The default administrative password is `admin`.

5 Enter a **New HTTP Administrative password**.

6 Enter the **HTTP User Name.**

7 Enter the **HTTP Password.**

8 Enter the **HTTP services IP filter masks**.

Examples:

- **Individual:** `190.200.100.10`
- **Multiple:** `190.200.100.10`
  `190.200.100.20`
- **Network:** `190.200.100.10/24b`

9 Enable the **Encrypt the HTTP settings file** option.

10 Click `Save Changes` to apply the new settings.

Viewing TermProxy Status and Sessions

This section provides information on TermProxy statistics, including the following:

- Viewing Session Status
- Suspending a Session
- Viewing Session List

Viewing Session Status

The TermProxy web interface gives you the ability to view and monitor specific session statistics, including:

- **Overall statistics**. These statistics include the software version, client and host connections and bytes sent and received.

- **Proxy-specific statistics**. These statistics include specific information about the Proxy Service and the Host Service. Proxy-specific statistics display for each TermProxy session running.

To view TermProxy status:

1 Access the TermProxy web interface.

2 From the *TermProxy Main Menu* page, click `Status`.

The *Current Status* page appears.

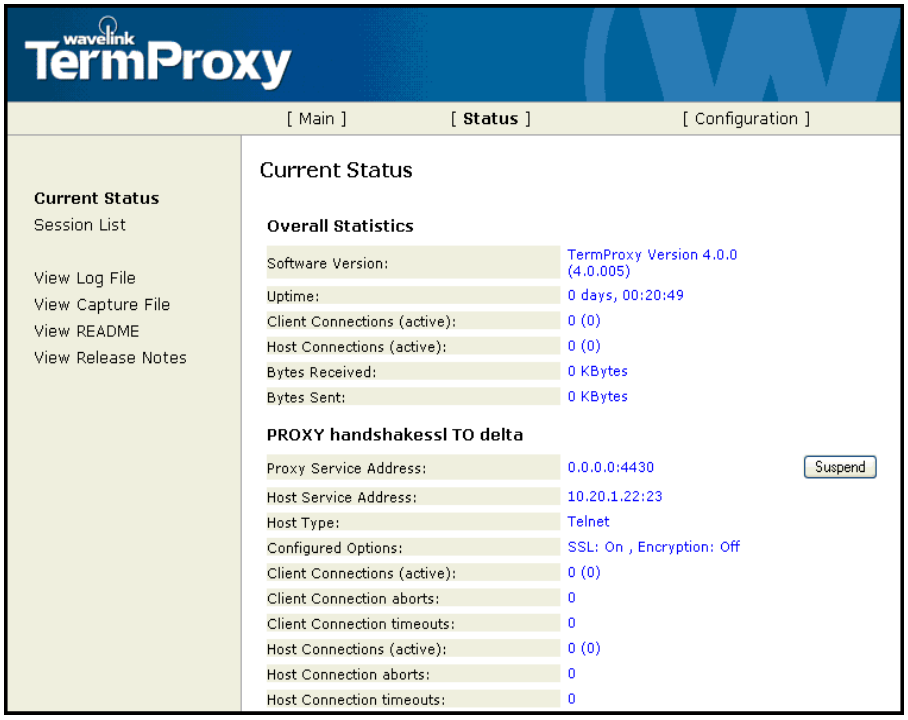

Figure 4-11. *Current Status Page*

The following table describes the Overall statistics.

Statistic	Description
Software Version	Displays the current version of TermProxy
Uptime	Displays the time elapsed since TermProxy was restarted.
Client Connections (active)	Displays the number of client connections. The first number displays the total number of connections that have been established since TermProxy was last restarted. The number in the parenthesis indicates the connections that are currently active.
Host Connections (active)	Displays the number of host connections. The first number displays the total number of connections that have been established since TermProxy was last restarted. The number in the parenthesis indicates the connections that are currently active.
Bytes Received	Total number of bytes received by both client and host.
Bytes Sent	Total number of bytes sent from both client and host.

Table 4-4: *TermProxy Overall Statistics*

The following table describes the proxy-specific statistics.

Statistic	Description
Proxy Service Address	Displays the proxyservice IP address for the specific session.
Host Service Address	Displays the hostservice IP address for the specific session
Host Type	Displays the type of host connection (Telnet or SSH).
Configured Options	Displays that state of the SSL/TLS configuration (on or off).
Client Connections (active)	Displays the number of client connections. The first number displays the total number of connections that have been established since TermProxy was last restarted. The number in the parenthesis indicates the connections that are currently active.
Client Connection aborts	Displays the number of times the client has aborted.
Client Connection timeouts	Displays the number of times the client has timed out.
Host Connections (active)	Displays the number of host connections. The first number displays the total number of connections that have been established since TermProxy was last restarted. The number in the parenthesis indicates the connections that are currently active.

Table 4-5: *TermProxy Proxy-Specific Statistics*

Statistic	Description
Host Connection aborts	Displays the number of times the host has aborted.
Host Connection timeouts	Displays the number of times the host has timed out.
Host Connection retries	Displays the number of times the host has attempted to reconnect.
Host Connection failures	Displays the number of times the host has failed to reconnect.
Host Bytes Received	Displays the number of byes received by the host.
Host Bytes Sent	Displays the number of bytes sent by the host.
Client Bytes Received	Displays the number of bytes received by the client.
Client Bytes Sent	Displays the number of bytes sent by the client.

Table 4-5: *TermProxy Proxy-Specific Statistics*

Suspending a Session

When you suspend a TermProxy session, new connections will not be allowed to connect to that proxyservice session until you resume the session. However, existing connections of a suspended proxyservice session are still functional.

To suspend or resume a session:

1. In the *Current Status* page, scroll to the session you want to suspend or resume.
2. Click the `Suspend` or `Resume` button to the right of the proxy session.

Viewing Session List

The *Session List* page of the TermProxy interface displays the following information about each active session:

- Client IP address
- Host name
- Connect time
- Last activity

If a stationid-template is used with AS/400 connections, you will see the workstation ID of the mobile device.

To view session list:

1 Access the TermProxy web interface.

2 From *TermProxy Main Menu* page, click `Status`.

The *Current Status* window appears.

3 In the left-channel navigation, click `Session List`.

The *Proxy Session* window appears.

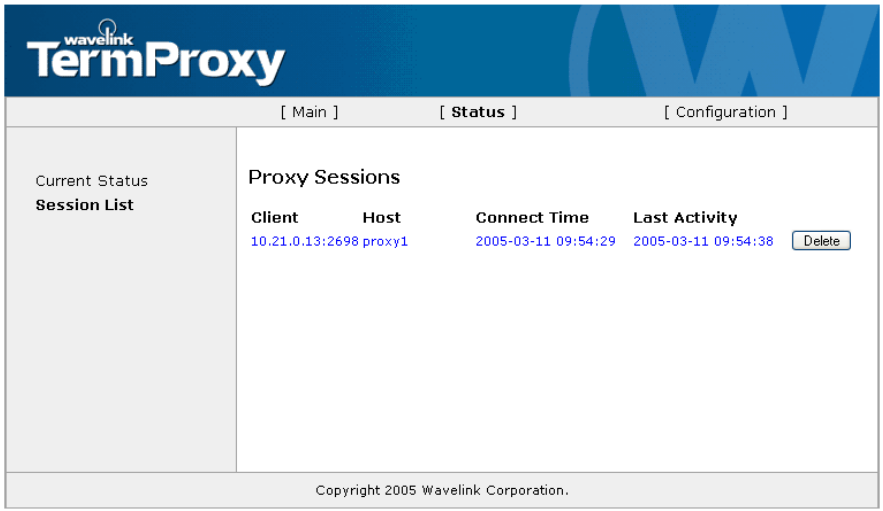

Figure 4-12. *Session List*

You can press the `Delete` button, located to the right of each session listing, to disconnect the TermProxy sessions.

Running TermProxy as a Service

The Win32 TermProxy product installation program installs the TermProxy server as a service. This section provides details about running TermProxy as a service. It contains the following information:

- Using TermProxy Command Line Switches
- Installing and Uninstalling the TermProxy Service

- Starting or Stopping the TermProxy Service

Using TermProxy Command Line Switches

You can use the `wltermproxyservice.exe` at the command line to configure TermProxy parameters.

To use the TermProxy switches:

1 On the host system, open the command prompt.

2 Use the command prompt to access the directory in which `wltermproxyservice.exe` is located.

3 Type `wltermproxyservice -h` to display the list of command line options.

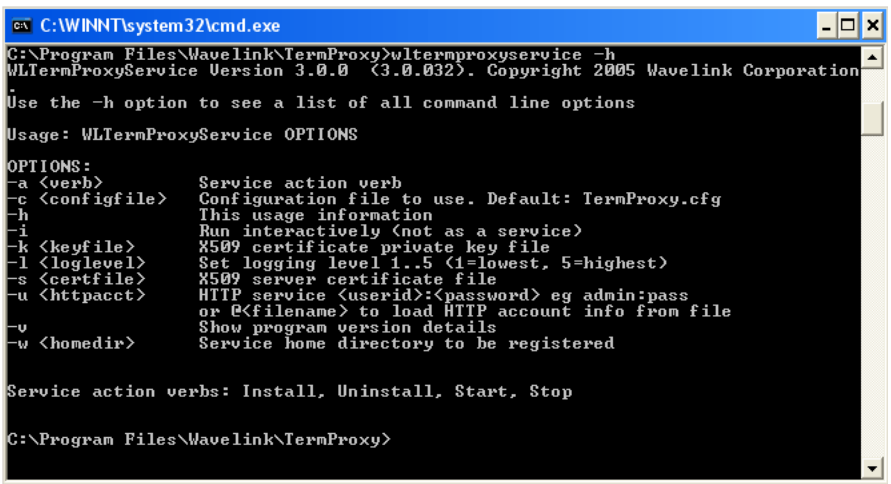

Figure 4-13. *Wltermproxyservice.exe Switches*

4 At the command line, `type wltermproxyservice [switch]`, where `[switch]` is the switch you want to apply to the command. The following table lists the available switches and describes their function.

Switch	Function
-a [*verb*]	Invokes a certain action, as specified by the [*verb*] parameter. The [*verb*] portion of the switch can be any of the following: **Install.** Installs the TermProxy as a service. **Uninstall.** Uninstalls the TermProxy service. **Start.** Starts the TermProxy service. **Stop.** Stops the TermProxy service. Example: `wltermproxyservice -a stop`
-c [*configfile*]	Specifies the configuration file that TermProxy uses, where `[configfile]` is the name of the configuration file. Example: `[-c c:\proxy\proxy.cfg]` Include the entire path with the file name if it is located in different directory than the default. Example: `[-c "c:\termproxy config\proxy.cfg"]` By default, TermProxy uses `TermProxy.cfg` within the directory where wltermproxyservice is installed.
-h	Displays a list of help options, which are described in this table.
-i	Causes TermProxy to run interactively, instead of as a service. This allows you access to the TermProxy console run-time functions, as described when you type `-h` for help in the command window. This should only used for testing.
-k [*keyfile*]	Indicates the X509 certificate private key file location. This option specifies the location of a pem key file to be used if the key file is not in the directory where the `wltermproxyservice.exe` resides. Example: `[-k c:\secure\skey.pem]`
-l [*loglevel*]	Sets the TermProxy logging level. The [*loglevel*] parameter is the logging level to which you want to set TermProxy. [*loglevel*] can be any number from 0 to 5 (0 being the lowest logging level). For more information about TermProxy logs, see *Logging and Data Capture* on page 66. This method does not allow *verbose* mode to be set.
-s [*certfile*]	Indicates the X509 server certificate file location. This option specifies the location of a pem certificate file to be used if certificate file is not in the directory where the `wltermproxyservice.exe` resides. Example: `[-s c:\secure\scert.pem]`

Table 4-6: *WLTermProxyService.exe Switches*

Switch	Function
-u [*httpacct*]	Indicates the TermProxy web server account user name and password on the command line. Example: `[-u <userid>:<password>]` Indicates a reference file that contains this information such as `http.cfg`. Example: `[-u@http.cfg] or [-u@c:\proxy\http.cfg]`
-v	Displays the TermProxy version information.
-w [*homedir*]	Specifies the home directory for TermProxy, where `[homedir]` is the path to the home directory. Use "`.`" to specify the current directory (that is, the directory from which WLTermProxyService is launched). Example: `[-w "c:termproxy folder"]`

Table 4-6: *WLTermProxyService.exe Switches*

Installing and Uninstalling the TermProxy Service

The `wltermproxyservice.exe` service is installed when you install the TermProxy product. The service is set to start automatically when the machine starts. Use `wltermproxyservice -a start` to start the service. You could also install the service using the command line `wltermproxyservice.exe -a install, -w.` and `-u@"c:\Program Files\Wavelink\TermProxy\http.cfg"`.

If you need to uninstall the TermProxy service, use `wltermproxyservice -a uninstall`. This will stop the service and then remove the service.

To reinstall the service, type `wltermproxyservice -ainstall, -w "c:\Program Files\Wavelink\TermProxy"`, and `-u@"c:\Program Files\Wavelink\TermProxy\http.cfg".` (The default installation path is presumed in the example.) Type `wltermproxyservice -a start` to start the TermProxy service.

Starting or Stopping the TermProxy Service

If you have installed TermProxy as a Windows service, you can start or stop the TermProxy service using the command line or from the Windows Services console.

To start or stop the TermProxy service from the Windows Services console:

1 Ensure that you have installed TermProxy as a service on the host system.

2 On the host system, access the Windows Control Panel.

3 In the *Control Panel*, access the **Administrative Tools**.

4 In **Administrative Tools**, double-click **Services**.

The *Windows Services* console appears in a new window.

5 In the *Services* console, locate and select the Wavelink TermProxy service.

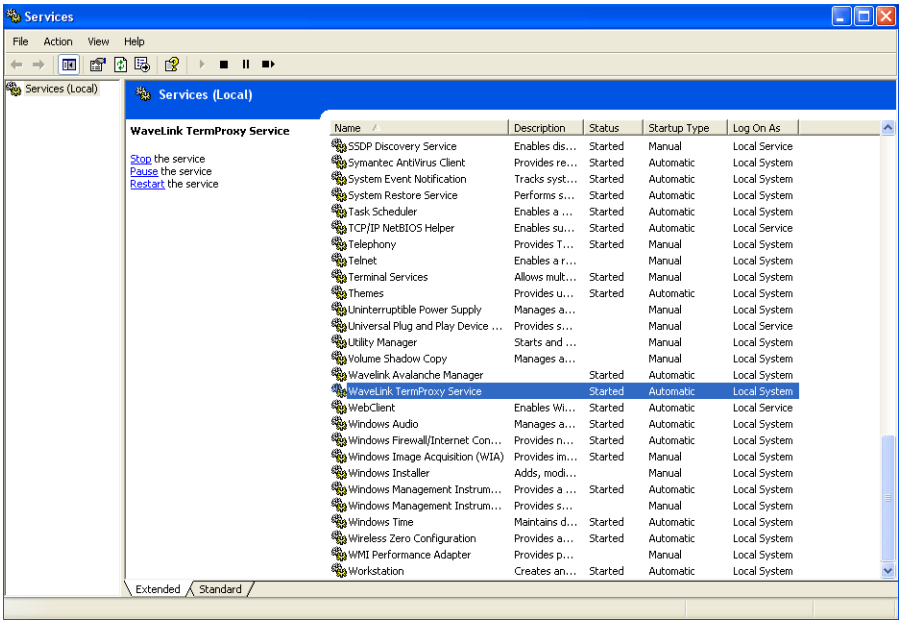

Figure 4-14. *Services Console*

6 Right-click the TermProxy service.

A drop-down list appears.

7 From the drop-down list, select `Start` or `Stop`.

The TermProxy service starts or stops.

To start or stop the TermProxy service from the command line:

1 Navigate to the directory where `wltermproxyservice.exe` resides.

2 Type `wltermproxyservice -a start` to start the service, or `wltermproxyservice -a stop` to stop the service.

Appendix A: Implementation Scenarios

The following section contains three different TermProxy implementation scenarios. Each scenario contains a network diagram, configuration parameters, and a brief discussion about the scenario.

Scenario 1: Multiple Clients to a Single Host

In Figure A-1, clients connect to a single host through a proxy server. This example is based on VT emulation with no reconnect string.

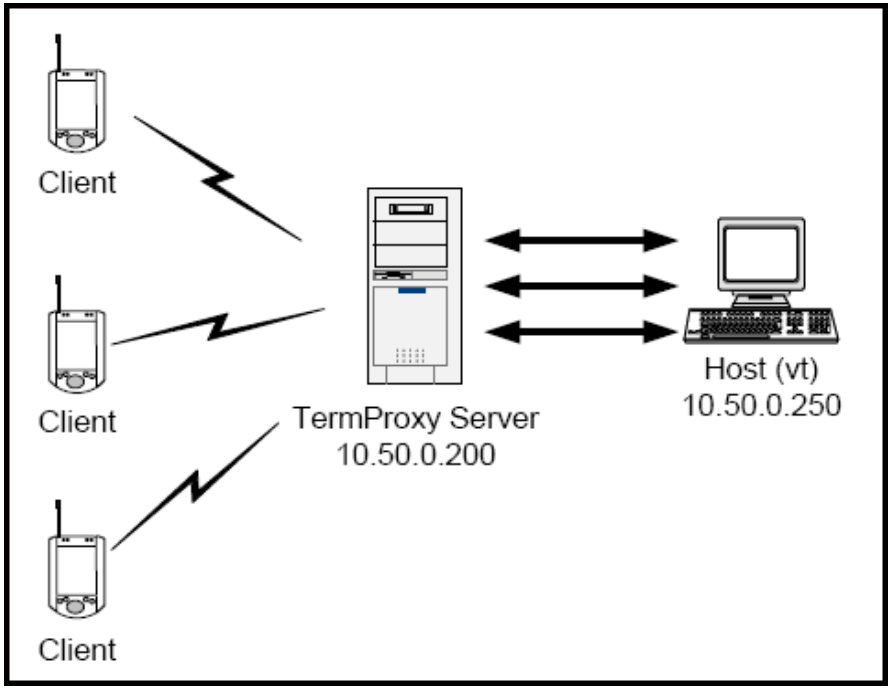

Figure A-1. *Multiple Clients Connect to a Single Host*

Configure the mandatory proxy parameters in the TermProxy configuration file as follows:

```
proxyservice proxy1
  listen 10.50.0.200:4430
  server VT
```

```
hostservice VT
  connect 10.50.0.250:23
```

Configure the TermProxy 1 entry within the host profile on the client to direct terminal emulation traffic to 10.50.0.200:4430.

Scenario 2: Multiple Clients to Multiple Hosts

In Figure A-2, clients can connect to one of three different hosts through a single proxy server. This example is based on VT emulation with no reconnect string.

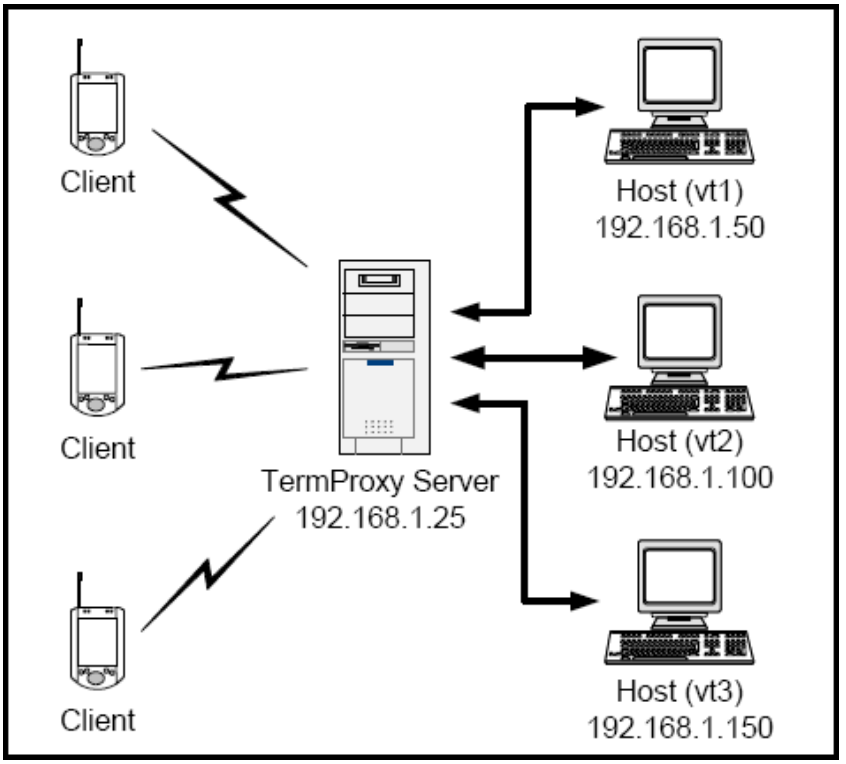

Figure A-2. *Multiple Clients Connect to Multiple Hosts*

Configure the mandatory parameters of the `termproxy.conf` file as follows:

```
proxyservice proxy1
  listen 192.168.1.25:4430
  server vt1, vt2, vt3

hostservice vt1
  connect 192.168.1.50:23

hostservice vt2
  connect 192.168.1.100:23

hostservice vt3
  connect 192.168.1.150

proxy       //proxy entry for connection to Host 1
  listen 192.168.1.25:2301
  server 192.168.1.50:23
```

Add three host profiles in the Telnet Client. Specify the TermProxy server in the TermProxy 1 tab of each host profile. The AS/400 release of TermProxy is typically used in this scenario.

Scenario 3: Multiple Clients to Proxy Server/Host

In Figure A-3, several clients connect to a system that hosts the Telnet service and the TermProxy application.

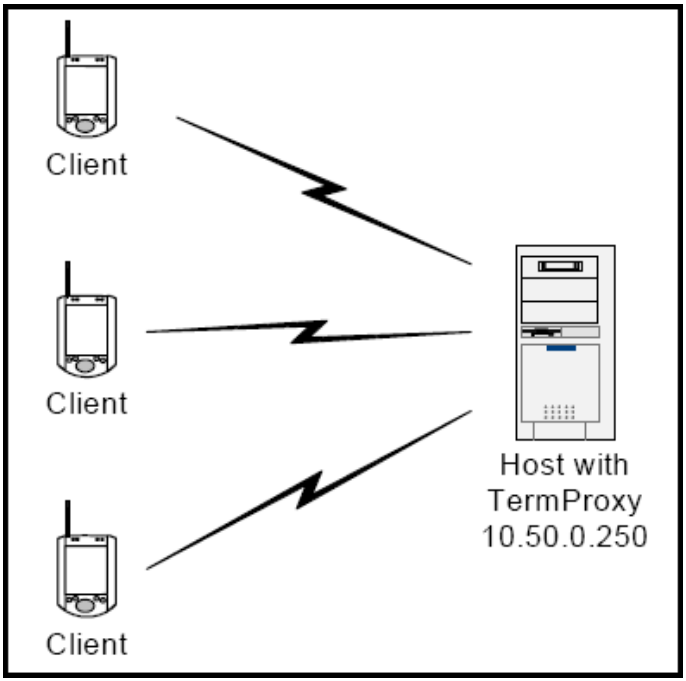

Figure A-3. *Multiple Clients Connect to a Proxy Server/Host*

Configure the proxy entry in the TermProxy configuration file as follows:

```
proxyservice proxy1
   listen 10.50.0.250:4430
   server as400

hostservice as400
   connect 10.50.0.250:23
   reconnect-string F3
   codeset EBCDIC
```

The clients need a host profile that directs session traffic to 10.50.0.250:4430.

Appendix B: Running TermProxy as a Console Application (Win 32 only)

This section provides details about running TermProxy as a console application. It includes the following information:

- Launching TermProxy
- Using TermProxy Command-Line Switches
- Using TermProxy Console Commands
- Closing TermProxy
- Uninstalling TermProxy

Launching TermProxy

If you have decided to use TermProxy as a console application (as opposed to a dedicated Windows service), you must manually launch the TermProxy application on the Win 32 system.

To launch TermProxy on the host system:

1. Install TermProxy using the InstallShield installation program.
2. Ensure that you have configured `termproxy.cfg` with the correct parameters to accommodate client and host connections.
3. On the host system, browse to the directory where you have installed the TermProxy components.
4. Double-click `Termproxy.exe`.

   TermProxy launches, and the application appears in its own command prompt.

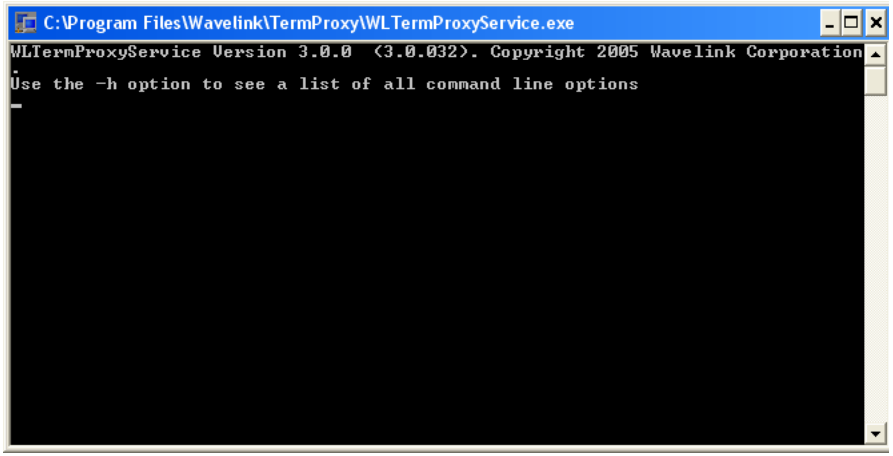

Figure B-1. *Running TermProxy as an Application*

Using TermProxy Command-Line Switches

`TermProxy.exe` has a number of switches that can be applied at the command line.While TermProxy is running, there are a number of switches you can use to invoke TermProxy commands. To invoke the switches, access the command prompt in which TermProxy is running, and then press the `Enter` key.

To use a command-line switch:

1 On the host system, open a command prompt.

2 Use the command line to access the directory in which `TermProxy.exe` resides.

3 At the command line, type `termproxy.exe [switch]`, where `[switch]` is the switch that you want to use (see Table B-1).

NOTE You can use more than one switch in the command. Commands ignore white space.

---

4 Type `termproxyservice -h` to display the list of command line options.

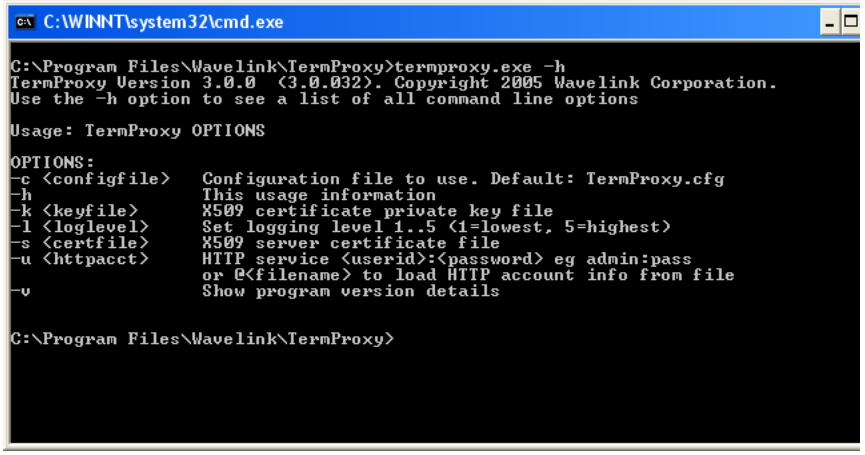

Figure B-2. *TermProxy Command Line Switches*

The following table shows the available command line switches and describes their function.

Switch	Function
-c [*configfile*]	Specifies the configuration file that TermProxy uses, where [*configfile*] is the name of the configuration file. Example: [`-c c:\proxy\proxy.cfg`]. Include the entire path with the file name if it is located in different directory than the default. Example: [`-c "c:\termproxy config\proxy.cfg"`]. By default, TermProxy uses TermProxy.cfg within the directory where `wltermproxyservice.exe` is installed.
-h	Displays the TermProxy help, which lists the available switches.
-k [*configfile*]	Indicates the X509 certificate private key file location. This option specifies the location of a pem key file to be used if the key file is not in the directory where the `wltermproxyservice.exe` resides. Example: [`-kc:\secure\skey.pem`]
-l [*level*]	Sets the TermProxy logging level. The [*loglevel*] parameter is the logging level to which you want to set TermProxy. [*loglevel*] can be any number from 0 to 5 (0 being the lowest logging level).This method does not allow verbose mode to be set. For information about logging, see *Table 4-3: TermProxy Logging Levels* on page 66

Table B-1: *TermProxy Command Line Switches*

Switch	Function
-s [*certfile*]	Indicates the X509 server certificate file location. This option specifies the location of a pem certificate file to be used if certificate file is not in the directory where the `wltermproxyservice.exe` resides. Example: [`-sc:\secure\scert.pem`]
-u [*httpacct*]	Indicates the TermProxy web server account user name and password on the command line. Example: [`-u<userid>:<password>`] Indicates a reference file that contains this information such as `http.cfg`. Example [`-u@http.cfg`] or [`-u@c:\proxy\http.cfg`]
-v	Displays the TermProxy version information.

Table B-1: *TermProxy Command Line Switches*

Using TermProxy Console Commands

While TermProxy is running, there are keys that you can press to invoke TermProxy commands. To invoke the command, access the command prompt in which TermProxy is running and then press the appropriate key.

NOTE You can also launch TermProxy from the command prompt. At the command line, browse to the directory and type `termproxy.exe`. TermProxy launches and runs from the command prompt in which you invoked the command.

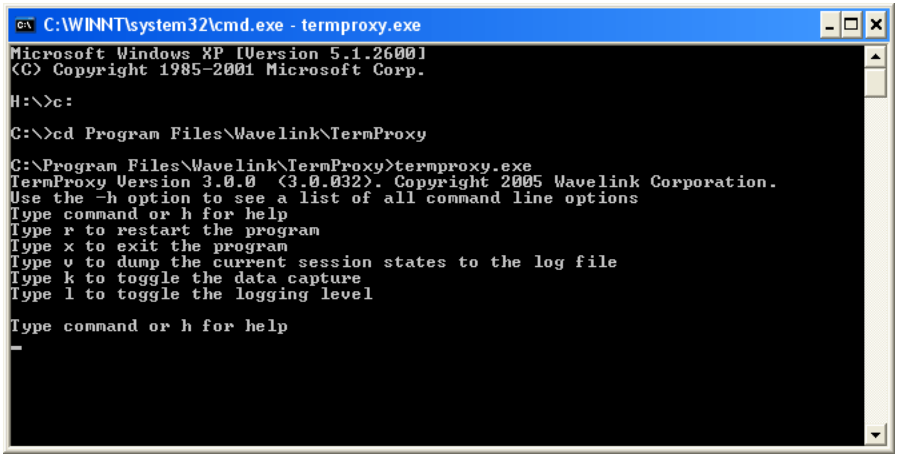

Figure B-3. *TermProxy Command Keys*

The following table lists the keys and their functions:

Key	Function
h	Calls up the help menu, which displays the TermProxy options that are available for the user (the options in this table).
r	Restarts TermProxy.
x	Exits TermProxy.
v	Dumps the current session states to the log file.
k	Toggles the data capture.
l	Toggles the logging level.

Table B-2: *TermProxy Commands*

Closing TermProxy

If you no longer need to use TermProxy, close the application from the command prompt.

To terminate the TermProxy application:

1 Access the command prompt in which TermProxy is running.

2 Type "x".

TermProxy closes. Any active Telnet sessions are disconnected. The command prompt also closes.

NOTE If you started TermProxy using the command line, then the command prompt does not close.

Uninstalling TermProxy

Uninstall the TermProxy service by typing `wltermproxyservice -auninstall` in the command prompt. This uninstall will stop the service and remove the program.

Appendix C: Wavelink Contact Information

If you have comments or questions regarding this product, please contact Wavelink Customer Service via email or telephone.

Email: customerservice@wavelink.com

Phone: 425-823-0111

Glossary

client Used to indicate a mobile device that is connecting to a host through a proxy server.

client-proxy session A communication session that has been established between a client and a proxy server.

comment delimiters A series of characters that are used to comment out text in the TermProxy configuration file.

connection Used to indicate a one-directional data flow from a client to a proxy server or from a proxy server to a host.

firewall An application or service that filters incoming and/or outgoing network traffic based on a set of user-configured rules. Most firewalls can filter data based on IP address, socket, and data state.

host Used to indicate a server to which clients connect, usually through a terminal emulation service such as Telnet.

host profile A host profile is a series of parameters, including an IP address and port number, that are loaded on a client. The host profile directs the client's communication to the correct host and TermProxy server.

hostservice entry A series of configuration parameters in the TermProxy configuration file that specify the parameters of the TermProxy hostservice session. A hostservice entry contains the IP address and port of the target host to which traffic is directed, the time-out value of a session, and (if necessary) a reconnect string.

httpserver A configuration in the TermProxy configuration file that specifies the IP address and port to which the TermProxy HTTP service binds itself

IP address Internet Protocol address. A virtual address that uniquely identifies a network connection.

log level A configuration in the TermProxy configuration file that specifies the amount of data TermProxy writes into the log file

mobile device Used to indicate any type of terminal or hand-held wireless device.

proxy.cfg A plain-text file in the AS/400 installation that the TermProxy application references for configuration information. This file tells the TermProxy on which ports to listen and where to redirect data flows.

proxyservice entry A series of configuration parameters in the TermProxy configuration file that specify the parameters of the TermProxy proxyservice session. A proxyservice entry contains the socket on which the proxy server listens, the host names to which traffic is directed, and SSL configuration.

proxy server Used to indicate a server or workstation that is hosting Wavelink TermProxy.

proxy-host session A communication session that has been established between a proxy server and a host.

RAM Random Access Memory. Volatile memory in a computer system.

readme.txt In the context of Wavelink TermProxy, a plain-text file that contains version information about the product.

reconnect string A series of characters that are used to resume work with a given host session.

session A bi-directional communication session between a client and a proxy server or between a proxy server and a host.

socket The combination of a unique IP address and a TCP or UDP port number. For example, 192.168.1.10:23.

SSH Secure Shell. A protocol that allows data to be sent over a secure channel.

SSL Secure Sockets Layer. A protocol that uses a private key to encrypt data and a configuration in the TermProxy configuration file that specifies if SSL encryption is used.

TCP/IP Transmission Control Protocol / Internet Protocol. A suite of communication protocols.

timeout value In the context of Wavelink TermProxy, a parameter that you must specify in a hostservice entry that indicates the amount of time the proxy server will maintain the proxy-host connection when the client-proxy session has gone idle or dead. If left unspecified in the TermProxy configuration file, it defaults to 15 minutes. Use minutes when you configure the time-out value in the configuration file. The time-out value is displayed in seconds when you run the TermProxy application.

Telnet An IP service that is used for terminal emulation. TCP port 23 is the standard port that is used for Telnet traffic.

TermProxy See *Wavelink TermProxy*.

termproxy.cfg A plain-text file in the Win 32 installation that the TermProxy application references for configuration information. This file tells the TermProxy on which ports to listen and where to redirect data flows.

TermProxy.exe The TermProxy application. Execute this file to launch the TermProxy application.

Wavelink TermProxy A proxy server that keeps the communication session between a client and a host for a user-configured amount of time, which allows clients to quickly resume terminal emulation even after the client has entered a sleep state or has otherwise experienced a communication disruption with the host.

Index

A

adding TermProxy configuration entries 31
AIX
  installation requirements 14
  installing TermProxy 22
  uninstalling TermProxy 26
AS/400
  installation requirements 13
  installing TermProxy 18
  reinstalling TermProxy 22
  uninstalling 25

C

command line switches 80, 81, 90
comment delimiters 38
configuration
  accessing TermProxy configuration 27
  adding TermProxy entries 31
  comment delimiters 38
  components 29
  creating TermProxy entries 31
  default 30
  format 31
  host profile 49, 50
  hostservice entry 33
  hostservice parameters 33
  httpserver 37
  httpserver parameters 37
  logging levels 67
  loglevel entry 36
  overview 27
  proxyservice entry 32
  proxyservice parameters 32
  reconnect strings 39, 40
  restarting 43
  samples 43
  saving 43
  Telnet Client 49
  TermProxy profile 51, 52
  translation table parameters 42
  validating entries 42
  VT escape sequence 40
  web interface 63
connections 8
console application
  closing 93
  commands 92
  launching 89
  running TermProxy 89
  uninstalling 94
console commands, using 92
contact information 95
creating TermProxy configurations 31

D

data capture
  enabling 70
  overview 67
  refreshing 72
  viewing 71
default TermProxy configuration 30
document
  assumptions 5
  conventions 6

F

features 9

H

host profile configuration 50
hostservice 33
http settings 73
  changing 74
  overview 73
httpserver parameters 37

I

implementation scenarios 85
- multiple clients to a single host 85
- multiple clients to multiple hosts 86
- multiple clients to proxy server/host 87

inserting verification certificates 61
installation 11
- AIX 22
- AS/400 18
- Linux 21
- obtaining 11
- requirements 12
- Windows 14

introduction 5

L

Linux
- installation requirements 14
- installing TermProxy 21
- uninstalling TermProxy 26

log file
- refreshing 72
- viewing 71

logging
- overview 67
- setting levels 68

logging levels 67
loglevel 36

M

multiple clients to a single host, implementation scenario 85
multiple clients to multiple hosts, implementation scenario 86
multiple clients to proxy server/host, implementation scenario 87

O

overview
- configuration 27
- data capture 67
- http settings 73
- logging 67
- TermProxy 6

P

proxyservice 32

R

readme file, viewing 64
reconnect strings
- 3270 reconnect string examples 40
- 5250 reconnect string examples 39
- configuring 39
- examples 39

reinstalling TermProxy 22
release notes, viewing 64
removing verification certificates 62
requirements, installation 12
restarting configurations 43
restarting TermProxy 65
run-time options 8

S

samples
- sample TermProxy configuration 1 parameter descriptions 44
- sample TermProxy configuration 2 parameter descriptions 45

saving configurations 43
session list, viewing 78
session status
- suspending sessions 78
- viewing 75

SSL/TLS
- creating new certificate 60
- deploying to the mobile device 56
- enabling support 58
- enabling verification 58
- inserting a certificate 61
- installing on the PC 56
- removing a certificate 62

statistics
suspending sessions 78
TermProxy overall statistics 77
TermProxy proxy-specific statistics 77
viewing session list 78
viewing session status 75

T

table statements, translate 42
Telnet Client
configuring host profile 49
configuring TermProxy profile 51
using TermProxy with 48
Telnet session, initiating with TermProxy 49
TermProxy
closing TermProxy as a console application 93
comment delimiters 38
configuration components 29
console commands 92
features 9
functionality 47
http settings 73
initiating Telnet session 49
installing as a service 82
introduction 5
launching TermProxy as console application 89
logging levels 67
obtaining installation 11
overview 6
proxyservice parameters 32
restarting 65
running as a console application 89
running as a service 79
run-time options 8
sample TermProxy entries 44, 45
sessions 75
starting service 82
statistics 77
status 75
stopping service 82
supported connections 8
table statement parameters 42
uninstalling as a service 82
uninstalling TermProxy as a console application 94
using 47
using with Telnet Client 48
web interface 63
translate table statements 42
translation table parameters 42

U

uninstalling TermProxy 24
AIX 26
AS/400 25
Linux 26
Windows 24
using
command line switches 80, 90
comment delimiters 38
TermProxy 47
TermProxy console commands 92
TermProxy with Telnet Client 48

V

validating configuration entries 42
verification certificates
creating 60
inserting 61
removing 62
viewing
readme file 64
release notes 64
session list 78
session status 75
VT escape sequences 40

W

Wavelink contact information 95
web interface
  accessing 64
  accessing TermProxy configuration 27
  changing http settings 74
  configuration 63
  data capture 71
  enabling data capture 70
  operations 63
  overview 64
  restarting TermProxy 65
  saving configurations 43
  suspending sessions 78
  validating TermProxy entries 42
  viewing log files 71
  viewing readme file 64
  viewing release notes 64
  viewing session list 78
  viewing session status 75
Windows 11
  installation 11
  installation requirements 12
  installing TermProxy 14
  running TermProxy as a console application 89
  uninstalling TermProxy 24
WLTermProxyService.exe switches 81