

Terminal Emulation

Wavelink ConnectPro Reference Guide

Version 4.4.1

Revised 17/05/2012

Copyright © 2012 by Wavelink Corporation All rights reserved.



Wavelink Corporation
10808 South River Front Parkway, Suite 200
South Jordan, Utah 84095
Telephone: (801) 316-9000
Fax: (801) 316-9099
Email: customerservice@wavelink.com
Website: <http://www.wavelink.com>

Email: sales@wavelink.com

No part of this publication may be reproduced or used in any form, or by any electrical or mechanical means, without permission in writing from Wavelink Corporation. This includes electronic or mechanical means, such as photocopying, recording, or information storage and retrieval systems. The material in this manual is subject to change without notice.

The software is provided strictly on an "as is" basis. All software, including firmware, furnished to the user is on a licensed basis. Wavelink grants to the user a non-transferable and non-exclusive license to use each software or firmware program delivered hereunder (licensed program). Except as noted below, such license may not be assigned, sublicensed, or otherwise transferred by the user without prior written consent of Wavelink. No right to copy a licensed program in whole or in part is granted, except as permitted under copyright law. The user shall not modify, merge, or incorporate any form or portion of a licensed program with other program material, create a derivative work from a licensed program, or use a licensed program in a network without written permission from Wavelink. The user agrees to maintain Wavelink's copyright notice on the licensed programs delivered hereunder, and to include the same on any authorized copies it makes, in whole or in part. The user agrees not to decompile, disassemble, decode, or reverse engineer any licensed program delivered to the user or any portion thereof.

Wavelink reserves the right to make changes to any software or product to improve reliability, function, or design.

The information in this document is bound by the terms of the end user license agreement.



Table of Contents

Chapter 1: Introduction	1
Functional Overview of ConnectPro	1
ConnectPro Features	2
Chapter 2: Installing the ConnectPro Server	3
Installation Requirements	3
Installing ConnectPro on Windows	3
Installing ConnectPro on Linux	4
Installing ConnectPro on AIX	5
Uninstalling ConnectPro	5
Chapter 3: Configuring the ConnectPro Server	7
Configuring ConnectPro with the Configuration Wizard	8
Configuring ConnectPro from the Text Window	10
Configuration Keywords	11
Proxy Service	11
Host Service	13
Log Level	15
Capture	16
Restart	16
HTTPserver	17
Configuring Reconnect Strings	18
Translating Table Statements	20
Validating Configuration Entries	21
Sample ConnectPro Configurations	21
Chapter 4: Configuring the Client for ConnectPro	25
Host Tab	25
TermProxy 1 Tab	27
Using SSL/TLS with ConnectPro	29
Using SSH with ConnectPro	29
Chapter 5: Using ConnectPro	30
Restarting the ConnectPro Server	31
Starting or Stopping the ConnectPro Service	32
Logging and Data Capture	33
Setting the Logging Level	34
Enabling Data Capture	35
Viewing Log and Capture Files	36
Viewing ConnectPro Status and Sessions	37
Viewing Session Status	37
Suspending a Session	39
Viewing Session List	40



Managing ConnectPro HTTP Settings	41
Deleting Stored Public Keys	43
Network Scenarios	44
ConnectPro as a Console Application	47
Wavelink Contact Information	50



Chapter 1: Introduction

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

ConnectPro (known in earlier versions as TermProxy) is designed to extend the life of sessions between Terminal Emulation Clients and hosts. Under normal operating circumstances, a device might go idle, enter power-saving mode, or move out of RF range and prematurely terminate the session between the Client and the host. ConnectPro server software maintains the session with the host, even if the device goes to sleep or the connection is momentarily lost. This enables the Client to seamlessly resume the session without loss of productivity.

This section provides the following information:

- [Functional Overview of ConnectPro](#)
- [ConnectPro Features](#)

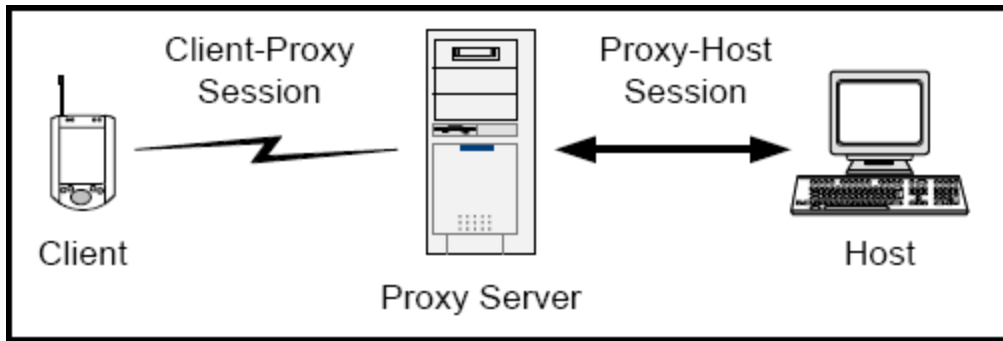
Functional Overview of ConnectPro

ConnectPro acts as an intermediary or proxy server between a Client and a host, maintaining an established session with the host even though the Client might go idle or otherwise terminate the session. The process occurs in the following manner:

- 1 The Client establishes a session with the proxy server. This is called the Client-proxy connection.
- 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 connection.
- 3 The proxy server maintains the proxy-host connection, even if the Client-proxy connection goes idle or dead. (You can configure the length of time that the proxy server maintains the proxy-host connection after the Client-proxy connection has 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. Block-mode emulations, such as 5250 and 3270, should use 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.





ConnectPro Process

ConnectPro Features

The following list describes additional features that ConnectPro offers:

- **Web Interface.** ConnectPro offers a web interface that allows you to configure ConnectPro, view log files, view data captures, delete Client-proxy or proxy-host sessions, and review the status of proxy services. Sessions with the ConnectPro web interface can be encrypted using SSL, TLS, or SSH.
- **Thousands of Concurrent Sessions.** ConnectPro can support a maximum of 5000 concurrent Client sessions. If you plan on supporting a large number of Clients (up to 5000), ensure that the host system meets the proper ConnectPro specifications. (For information on host system requirements, see [Installation Requirements](#) on page 3.) ConnectPro and the Client can be configuring with timeout or terminate-on-exit options that may help free up unused or idle connections.
- **Suspend/Resume Host Services.** ConnectPro allows you to suspend additional connections to the proxy service. All current connections remain functional, but new connections are denied until you resume the service.
- **Multiple Proxy Sessions per Client.** ConnectPro supports multiple proxy sessions for each device.
- **SSL, TLS, or SSH Support.** ConnectPro supports SSL/TLS or SSH for encryption and verification when connecting to the web interface or for Client-proxy connections.
- **Data Capture Filter.** ConnectPro can capture data from a single Client, from multiple Clients, or from all Clients. Captured data is stored in a text file on the proxy host system. View the text file either manually or through the ConnectPro web interface.
- **Retrieve/Display IBM Workstation ID.** Configure ConnectPro 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 ConnectPro interface. (This applies only to Clients that are attempting to connect to an IBM AS/400 system.)



Chapter 2: Installing the ConnectPro Server

ConnectPro is available for Microsoft Windows 7, Windows 2003 or 2008 Server, Windows XP Professional, Linux, and AIX. All files required to install and operate ConnectPro can be obtained from the Wavelink Web site.

This chapter provides the following information:

- [Installation Requirements](#)
- [Installing ConnectPro on Windows](#)
- [Installing ConnectPro on Linux](#)
- [Installing ConnectPro on AIX](#)
- [Uninstalling ConnectPro](#)

NOTE: This version of ConnectPro is not supported on AS/400 servers. To install on AS/400, Wavelink recommends TermProxy 3.x.

Installation Requirements

This section provides information about the requirements for the system that will host ConnectPro. ConnectPro can be installed on one of the following operating systems: Microsoft Windows 7, Windows 2003 or 2008 Server, Windows XP Professional, Linux, and AIX.

The host system should also meet the following requirements:

- Intel Pentium 4 2.4 GHz (or equivalent) processor
- 512 MB RAM if you plan to use less than 1000 TE Clients; 1 GB RAM if you plan to use more than 1000 Clients. Each Client-to-host connection through ConnectPro requires approximately 64 KB of RAM per session.
- 50 MB disk space. ConnectPro requires additional hard disk space to support the log file. For additional information about the ConnectPro log file, see [Logging and Data Capture](#) on page 33.

NOTE: Wavelink recommends that if you are supporting more than 1000 Clients, you use a dedicated server to host ConnectPro.

Installing ConnectPro on Windows

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



To install ConnectPro:

- 1 Obtain and save the ConnectPro installation program to the target host system.

- 2 Double-click the executable to launch it.

The *Wavelink TermProxy Setup Wizard* appears.

- 3 Click **Next**.

The *License Agreement* dialog box appears.

- 4 Click **I Agree** to accept the terms of the license agreement.

The *Choose Install Location* dialog box appears.

- 5 Click **Install** to accept the default installation location, or click **Browse** to navigate to a folder of your choice.

- 6 After you click **Install**, the ConnectPro server installs. A dialog box appears asking if you want to add a shortcut to the desktop. Click **Yes** to add a shortcut to the desktop, if desired.

- 7 The installer launches the ConnectPro TermProxy initial installation configuration wizard in a web browser, and a dialog box appears asking if you want to set the MaxUserPort value to increase the number of sessions possible. (This allows each Client to maintain four concurrent sessions.) If you click **Yes**, the following registry key is added to the computer's registry:

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

- 8 The Completing the Wavelink TermProxy Setup Wizard screen appears. Click **Finish** to close the wizard, and follow the steps in [Configuring ConnectPro with the Configuration Wizard](#) on page 8 in order to configure the ConnectPro server.

Installing ConnectPro on Linux

This section contains information about one method for installing ConnectPro on a Linux operating system. You must have root user privileges to install or run ConnectPro.

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

To install ConnectPro on Linux:

- 1 Download the `.rpm` installation file.
- 2 Enter the following commands at the terminal:




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

ConnectPro is installed on the host system. The installer launches the ConnectPro TermProxy initial installation configuration wizard in a web browser. Follow the steps in [Configuring ConnectPro with the Configuration Wizard](#) on page 8 in order to configure the ConnectPro server.

- 3 To start ConnectPro, use the following command:

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

- 4 To stop ConnectPro, use the following command:

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

Installing ConnectPro on AIX

This section contains information about one method for installing ConnectPro on an AIX operating system. You must have root user privileges to install or run ConnectPro. There are alternate methods for installing ConnectPro on AIX. You may use a different installation method if desired.

[To install ConnectPro 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.

ConnectPro is installed on the host system. The installer launches the ConnectPro TermProxy initial installation configuration wizard in a web browser. Follow the steps in [Configuring ConnectPro with the Configuration Wizard](#) on page 8 in order to configure the ConnectPro server.

Uninstalling ConnectPro

This section provides instructions for uninstalling ConnectPro.

[To uninstall ConnectPro:](#)

- Click **Start > Programs > Wavelink TermProxy > Uninstall TermProxy**.

ConnectPro is removed from the host system.



To uninstall ConnectPro from Linux:

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

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

ConnectPro is removed from the host system.

To uninstall ConnectPro from AIX:

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

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

ConnectPro is removed from the host system.



Chapter 3: Configuring the ConnectPro Server

Configure the ConnectPro server after installation from the web interface. The web interface allows you to define the Client-proxy and host-proxy connections, modify the ConnectPro web server connection information, and modify the logging level.

To access the web interface:

- 1 Open a web browser and type the address and port of the ConnectPro web server in the address bar.

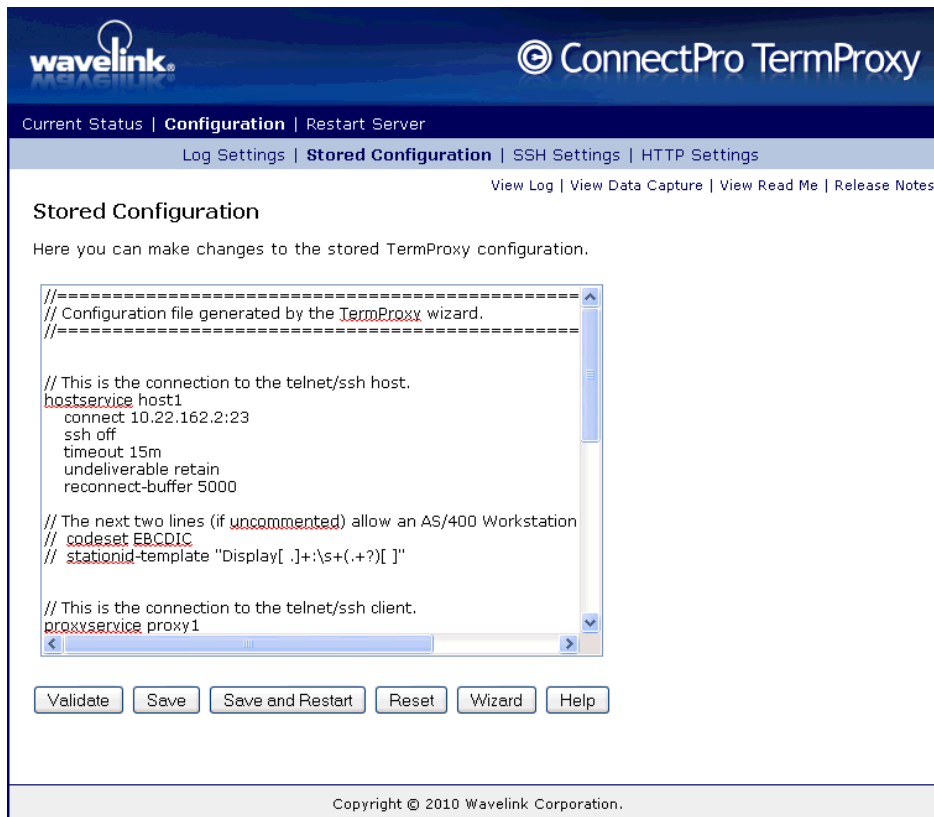
Example: `http://192.168.1.10:4428`

- 2 The *Authentication Required* dialog box appears. Enter the user name and password in the provided text boxes and **OK**.

NOTE: This is the password set in the initial configuration when ConnectPro was installed.

The *Current Status* page appears. Click **Configuration** in the navigation bar across the top.

The *Stored Configuration* page appears.



The screenshot shows the 'Stored Configuration' page in the ConnectPro TermProxy web interface. The page has a dark blue header with the 'wavelink' logo and 'ConnectPro TermProxy' text. Below the header is a navigation bar with 'Current Status', 'Configuration', and 'Restart Server'. The 'Configuration' section includes 'Log Settings', 'Stored Configuration', 'SSH Settings', and 'HTTP Settings'. There are links for 'View Log', 'View Data Capture', 'View Read Me', and 'Release Notes'. The main content area is titled 'Stored Configuration' and contains the text: 'Here you can make changes to the stored TermProxy configuration.' Below this is a text area containing a configuration file with the following content:

```
//=====
// Configuration file generated by the TermProxy wizard.
//=====

// This is the connection to the telnet/ssh host.
hostservice host1
  connect 10.22.162.2:23
  ssh off
  timeout 15m
  undeliverable retain
  reconnect-buffer 5000

// The next two lines (if uncommented) allow an AS/400 Workstation
// codeset EBCDIC
// stationid-template "Display[.]+\s+(.+)[ ]"

// This is the connection to the telnet/ssh client.
proxyservice proxy1
```

At the bottom of the text area are buttons for 'Validate', 'Save', 'Save and Restart', 'Reset', 'Wizard', and 'Help'. The footer of the page reads 'Copyright © 2010 Wavelink Corporation.'

Stored Configuration Page



This page provides options for configuring the ConnectPro server. You can change values in the text window or click **Wizard** to launch the Configuration Wizard, which provides additional help in configuring ConnectPro.

- For a description of options available in the text window, see [Configuring ConnectPro from the Text Window](#) on page 10.
- For information on using the Wizard, see [Configuring ConnectPro with the Configuration Wizard](#) on page 8.

In addition to modifying and saving the configuration (either through the text window or the Wizard), this page gives you the option to **Validate** the changes you've made, **Save and Restart** the server with the changes applied, or **Reset** the page to the last saved configuration. Pushing the **Help** button provides details about configuring the server using the text window.

For examples of how to configure ConnectPro, see [Sample ConnectPro Configurations](#) on page 21.

Configuring ConnectPro with the Configuration Wizard

When you install ConnectPro, the installer uses a web browser to open a Configuration Wizard that allows you to configure the ConnectPro server. You can also access the Configuration Wizard from the ConnectPro web interface.

NOTE: The Configuration Wizard is a simplified method of configuring ConnectPro. For advanced configuration options, see [Configuring ConnectPro from the Text Window](#) on page 10.

To configure ConnectPro from the Configuration Wizard:

- 1 Open the Configuration Page in the ConnectPro web interface and click **Wizard**. For details on accessing this page, see [Configuring the ConnectPro Server](#) on page 7.
- 2 In the Configuration Wizard, on the Step 1: Host Service page, provide the following information:
 - **Host Address.** The address of the emulation host(s) that the ConnectPro Server will be supporting.
 - **Host Port(s).** The port or ports used by the emulation host.
 - **The host uses SSH (instead of Telnet).** When the host and ConnectPro server use SSH, the information transmitted between them is encrypted.
 - **Timeout.** The amount of time the ConnectPro server will wait after a Client has been disconnected before it will disconnect the proxy-host session.



- **Terminate the connection if the host sends data while no client is connected to TermProxy.** This option disconnects the proxy-host connection if the Client is unavailable for information sent from the host.
- **Reconnect String.** Sends a specific keypress to the host when the Client reconnects. For example, the Client can send a keypress that will navigate to a main menu when the Client reconnects.

When you have configured the options, click **Next**.

3 The Step 2: Proxy Service page appears. Configure the following options:

- **Proxy Address.** The address the ConnectPro server will bind to. You can specify a proxy address of `0.0.0.0` if you do not want to limit the network interfaces ConnectPro can use.
- **Proxy Port.** The port that the Clients use to connect to the ConnectPro server.
- **Timeout.** The amount of time the ConnectPro server will wait after a Client has been disconnected before it will disconnect the proxy-host session.
- **Clients may connect through a Network Access Translation (NAT) device.** Enable this option to ensure that sessions are not disconnected prematurely when using a NAT device.

When a Client connects to ConnectPro, the ConnectPro server checks to see if there are any sessions for the Client's IP address. If the Client is not aware of any saved sessions, ConnectPro will, by default, close any sessions using the same IP address. However, if multiple clients can have the same IP address, sessions for other Clients could be closed prematurely when a new Client connects. When this option is enabled, ConnectPro will not close current sessions.

- **Compress data sent to newer Clients.** This option compresses any block of data larger than 500 bytes sent to Clients that are version 7.2.12 or newer. You can have compression enabled when using Clients older than 7.2.12, but the data sent to those Clients will not be compressed.
- **Encryption.** This encrypts the session between the ConnectPro Server and the Client. If you are using SSH, you must change this setting. Available options are SSL/TLS, and Custom Encryption (a proprietary Wavelink encryption method).
- **Custom Encryption Passphrase.** If you use Custom Encryption, provide a passphrase to be used between the Client and the ConnectPro server. This should match the custom encryption passphrase supplied to the Client in the emulation parameters.

When you have configured the options, click **Next**.

4 The Step 3: HTTP Server page appears. Configure the following options:



- **HTTP Address.** This is the address or range of addresses allowed to access the ConnectPro web interface.
- **HTTP Port.** The port that the HTTP server listens on for requests to access the web interface.
- **HTTP User Name.** A user name required to access the web interface.
- **HTTP/Administrative Password.** A password required to access the web interface.
- **Use HTTPS (SSL) instead of HTTP (clear).** This encrypts the connection when you are connected to the ConnectPro server using a web browser.

When you have configured the options, click **Next**.

- 5 The Step 4: Other Settings page appears. Configure the following options:
 - **Logging Level.** This sets the logging level for the ConnectPro server. Options include **Errors**, **Warning**, **Info**, and **Debug**.
 - **Restart Time(s).** The time(s) of day you want the ConnectPro server to automatically restart. Each time needs to follow the format HH:MM[a|p]. If there is no 'a' or 'p' following the time (representing AM or PM), the time is assumed to be in a 24-hour format. Specify a weekly time (instead of a daily time) by preceding the time with the day of the week. All times are local times, and will use the time zone value of the computer running ConnectPro.

Examples:

SU02:00A, M02:10A, TU02:20A, W02:30A, TH02:40A, F02:50A, SA03:00A

MONDAY22:30, THURSDAY00:30

When you have configured the options, click **Finish**.

- 6 The Wizard Completed screen appears and the ConnectPro server starts running. XXX does it startup here or earlier? When do these changes get applied? XXX

Configuring ConnectPro from the Text Window

There are features of the ConnectPro server that are not configurable using the Configuration Wizard. In order to configure these options, you should use the text window on the *Stored Configuration* page in the web interface. You can also use the text window to configure ConnectPro to connect to multiple hosts with different encryption levels or connection options.



When you use the text window to configure the ConnectPro server, each configuration is specified by keyword/value pairs separated by white space (either spaces or tabs). If a value (such as a passphrase) contains a space, the entire value should be enclosed in quotation marks (" "). The keywords and values are not case-sensitive, but each pair should begin on its own line. You may use # or // to indicate that the remainder of the line is a comment.

The following information is provided:

- [Configuration Keywords](#)
- [Configuring Reconnect Strings](#)
- [Translating Table Statements](#)
- [Validating Configuration Entries](#)

Configuration Keywords

This section contains information about the format and parameters of the ConnectPro stored configuration. The configuration information is entered in keyword/value pairs, and the entries are organized into the following sections:

- [Proxy Service](#)
- [Host Service](#)
- [Log Level](#)
- [Capture](#)
- [Restart](#)
- [HTTPserver](#)

Proxy Service

A proxy service entry defines the connections between the Clients and the ConnectPro server. You must have at least one proxy service defined. Use the following format to create a proxy service entry in the ConnectPro configuration:

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

The following table contains detailed information about each parameter in the proxy service entry:



Parameter	Description
<code>proxyservice</code> [<i>proxyservice</i> <i>name</i>]	Specify a name for the proxy service. The name is used in the ConnectPro user interface and log file. This is a required parameter.
<code>listen</code> [<i>ipaddr:port</i>]	Specify the interface and port number on which the proxy server should listen for Client connections. Use <code>0.0.0.0</code> to specify that the proxy server should listen for a specific port number on all local interfaces. For example, the value <code>0.0.0.0:2301</code> instructs ConnectPro to listen for Client connections on port 2301 for all local interfaces on the ConnectPro server. This is a required parameter.
<code>server</code> [<i>hostservice</i>]	Specify the host service names to be associated with a proxy service. 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. An asterisk (*) can be specified as the host service name. ConnectPro will then allow the Client to establish sessions with arbitrary applications, whether they are configured with a host service statement or not. This should not be used when ConnectPro is reachable through a firewall or is located in a DMZ. This is a required parameter.
<code>timeout</code> [<i>time</i>]	Specify the amount of time before ConnectPro terminates the Client-proxy session due to inactivity (also referred to as the Client timeout). Specify a value of <code>0</code> 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 ConnectPro 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 or 24h or 1440m or 86400s). This parameter is optional and will default to <code>24h</code> .
<code>ssl</code> [<i>on</i> <i>off</i>]	Set this value to <code>on</code> to use the Secure Sockets Layer (SSL) protocol to communicate with the browser. ConnectPro 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 <code>off</code> .
<code>encryption</code> [<i>passphrase</i>]	Specify an encryption key to use custom encryption for Client connections.



NOTE: You cannot define a connection to support both SSL and custom encryption.

Host Service

A host service entry defines the connections between the ConnectPro server and the host(s). Use the following format to create a host service entry in the ConnectPro configuration:

```
hostservice [hostservicename]
connect [ipaddr:port]
ssh [on | off]
ssh-verify [on | off]
timeout [min]
reconnect-string [reconnect-string]
reconnect-buffer [size]
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 host service entry.

Parameter	Description
hostservice [hostservicename]	Specify a name for the host service. The name is used in the ConnectPro 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 host service, 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 <code>on</code> or <code>off</code> to determine whether ConnectPro uses SSH encryption for the proxy-host session.
ssh-verify [on off]	Specify either <code>on</code> or <code>off</code> to determine whether to allow Client-host connections when the public key does not match the expected key.



Parameter	Description
	If <code>off</code> is specified, the Client-host connection will be allowed and warning messages will be sent to the Client.
<code>timeout [min]</code>	<p>Specify the amount of time before ConnectPro terminates the proxy-host session. Specify a value of <code>0</code> to allow sessions to remain open indefinitely.</p> <p>This time begins once the Client-proxy connection closes (after the Client timeout expires).</p> <p>This parameter is optional and will default to <code>15m</code>.</p>
<code>reconnect-string [string]</code>	<p>A reconnect string requests the last screen data that the host had before the mobile device disconnected. Input a reconnect string or use one you defined in the ConnectPro configuration file. The reconnect string in the host profile takes precedence over the reconnect string in the ConnectPro configuration file.</p> <p>Requirements for connect strings depend upon the application, but the strings are required in 5250 and 3270 environments. For more information on reconnect strings, see Configuring Reconnect Strings on page 18.</p>
<code>reconnect-buffer [size]</code>	<p>Specify a value to determine the maximum amount of host-to-Client data (in bytes) that will be saved when a Client reestablishes a connection with ConnectPro.</p> <p>This option is only available if no <code>reconnect-string</code> is specified.</p>
<code>undeliverable [DISCARD ABORT]</code>	<p>Specify either <code>DISCARD</code> or <code>ABORT</code> for sessions with a host connection, but no current Client connection. <code>DISCARD</code> will delete unsolicited outbound data sent by the host application. <code>ABORT</code> will terminate the host connection.</p> <p>This parameter is optional and will default to <code>DISCARD</code>.</p>
<code>codeset [ASCII EBCDIC]</code>	<p>Specify <code>ASCII</code> or <code>EBCDIC</code> to determine how ConnectPro searches the application data for a station ID and how it presents capture file records.</p> <p>Select <code>EBCDIC</code> when using 5250 and the <code>stationid-template</code>.</p> <p>This parameter defaults to <code>ASCII</code>.</p>
<code>stationid-</code>	Specify the <code>stationid-template</code> .



Parameter	Description
template [<i>regular expression</i>]	<p>The stationid-template 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.</p> <p>Example: Display [.]+:\s+(.+?) []</p> <p>This is an optional parameter and configured only with the 5250.</p>
translate-tohost [<i>tablename</i>]	<p>ConnectPro 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.</p> <p>For more information, see Translating Table Statements on page 20.</p> <p>This parameter is optional and defaults to No translation.</p>
translate-fromhost [<i>tablename</i>]	<p>Specify the mapping tables for the outbound data stream.</p> <p>ConnectPro provides a simple byte-replacement mechanism for the outbound data stream. For more information, see Translating Table Statements on page 20.</p> <p>This parameter is optional and defaults to No translation.</p>

Log Level

Use the following format to create a log level entry in the ConnectPro configuration:

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

The following table contains detailed information about the loglevel entry.

Parameter	Description
loglevel [<i>logging level</i>]	<p>Specify the log level. The log level controls the amount of data ConnectPro 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.</p> <p>This configuration setting is meant to be the 'normal' setting for the day-to-day operation. The <i>Logging and Data Capture Settings</i> page in the ConnectPro Web interface allows you to temporarily change that level setting.</p>



Parameter	Description
	<p>The following is a list of the log level settings. The numbers in parentheses can be used in place of the name.</p> <p>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 logging information</p>

Capture

ConnectPro can capture proxy communication information. Use the following format to create a capture entry in the ConnectPro configuration:

```
capture [on |off]
clear [on | off]
include [filter]
```

The following table contains detailed information about the capture entry.

Parameter	Description
capture [on off]	Specify either <code>on</code> or <code>off</code> to determine whether proxy communication data is captured.
clear [on off]	Specify either <code>on</code> or <code>off</code> to determine whether the data capture file is emptied when ConnectPro starts or restarts.
include [filter]	<p>Specify a comma-delimited list of Client IP addresses that will have their data captured.</p> <p>Use the format <code>x.x.x.x/y</code> to specify an entire subnet.</p> <p>Example: <code>10.0.0.0/8</code> indicates addresses 10.0.0.0 to 10.255.255.255.</p> <p>Do not use the <code>include</code> parameter if you want to capture the network traffic for all devices.</p>

Restart

Use the following format to create a restart entry in the ConnectPro configuration:

```
restart [restart time]
```

The following table contains detailed information about the restart entry.



Parameter	Description
restart [time]	<p>Specify a comma-delimited list of times that ConnectPro will automatically restart.</p> <p>Enter times using the following format: HH:MM[a p]. If there is no 'a' or 'p' following the time (representing AM or PM), the time is assumed to be in a 24-hour format. Specify a weekly time by preceding the time with the day of the week.</p> <p>Examples: 10:00P, 06:00A, MONDAY22:30</p> <p>This is a required parameter.</p>

HTTPserver

Use the following format to create an `httpserver` entry in the ConnectPro configuration:

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

The following table contains information about the `httpserver` entry.

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



Configuring Reconnect Strings

To configure a reconnect string, 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 reconnect strings for 5250 emulation.

- 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 reconnect strings for 3270 emulation.

- 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 Sequences

The following are examples of escape sequences for VT emulation.

- 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 list provides some common VT escape values.

%00 Ctrl-A

%01 Ctrl-B

%02 Ctrl-C

%03 Ctrl-D

%04 Ctrl-D

%05 Ctrl-E

%06 Ctrl-F

%07 Ctrl-G a.k.a. Bell

%08 Ctrl-H a.k.a. Backspace

%09 Ctrl-I a.k.a. Tab

%0A Ctrl-J a.k.a. Line Feed or Newline

%0B Ctrl-K

%0C Ctrl-L a.k.a. Form Feed or Redraw Screen

%0D Ctrl-M a.k.a. 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 ConnectPro configuration:

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

The following table contains information about the table statement entry.

Parameter	Description
table name	This is a freely chosen name for the table. The host service 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.

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 ConnectPro configurations, validate your entries to ensure accuracy.

To validate configuration entries:

- Click the **Validate** button at the bottom of the Stored 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.

Sample ConnectPro Configurations

The following samples display ConnectPro configurations and detailed descriptions of the parameters used.

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 describes the parameters in Sample Configuration 1.

Sample Configuration	Description
proxyservice TelnetOne	The proxy service name is TelnetOne.
listen 0.0.0.0:2301	The proxy service listens for mobile devices on any local IP interface with 2301 as the listen port.
server TelnetHost	The proxy service interfaces with the host service named TelnetHost.



Sample Configuration	Description
timeout 5	The Client-proxy connection will time out after five minutes of inactivity.
ssl on	Mobile devices must use SSL to access a host service using the TelnetOne proxy service.
hostservice	The host service name is TelnetHost. TelnetHost is referenced within the proxy service TelnetOne.
connect 192.168.1.1:23	When a mobile device connects to the proxy service "TelnetOne" using the a host profile that contains 192.168.1.1:23, the ConnectPro establishes a connection with the target host 192.168.1.1:23.
timeout 1h	Once the client-proxy connection times out, the proxy-host connection starts counting down. It times out 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.

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 describes the parameters in Sample Configuration 2.



Sample Configuration	Description
<code>proxyservice TelnetHosts</code>	The proxy service name is TelnetHosts.
<code>listen 20.30.40.50:4430</code>	The proxy service listens for mobile devices at 20.30.40.50 and port 4430.
<code>server "Host AS400", "Host VT"</code>	The proxy service services two host services named "Host AS400" and "Host VT".
<code>hostservice "Host AS400"</code>	The first host service name is "Host AS400".
<code>connect 206.125.145.25:23</code>	When a mobile device connects to the proxy service "TelnetHosts" using the a host profile that contains 206.125.145.25:23, the ConnectPro server establishes a connection with the target host 206.125.145.25:23.
<code>reconnect %00%0D%12%A0%00%00%04%00%00%03%01%01%33%FF%EF</code>	This reconnect string sends an F3 upon reconnect.
<code>codeset EBCDIC</code>	The EBCDIC codeset allows the workstation ID to display in the Session List page of the ConnectPro web interface.
<code>stationid-template "Display [.] +:\s+ (.t?) []"</code>	The stationid-template allows the workstation ID to display in the <i>Session List</i> page of the ConnectPro web interface.
<code>hostservice "Host VT"</code>	The second host service name is "Host VT".
<code>connect 207.95.165.10:23</code>	When a mobile device connects to the proxy service "TelnetHosts" using the a host profile that contains 207.95.165.10:23, the ConnectPro establishes a connection with the target host 207.95.165.10:23.



Sample Configuration	Description
log level INFO	The log level entry instructs the proxy server to log information at the INFO level only.
httpservice 201.120.140.10:4428	The http service 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.

Timeout is not specifically defined in this sample configuration. This parameter defaults to 24 hours.



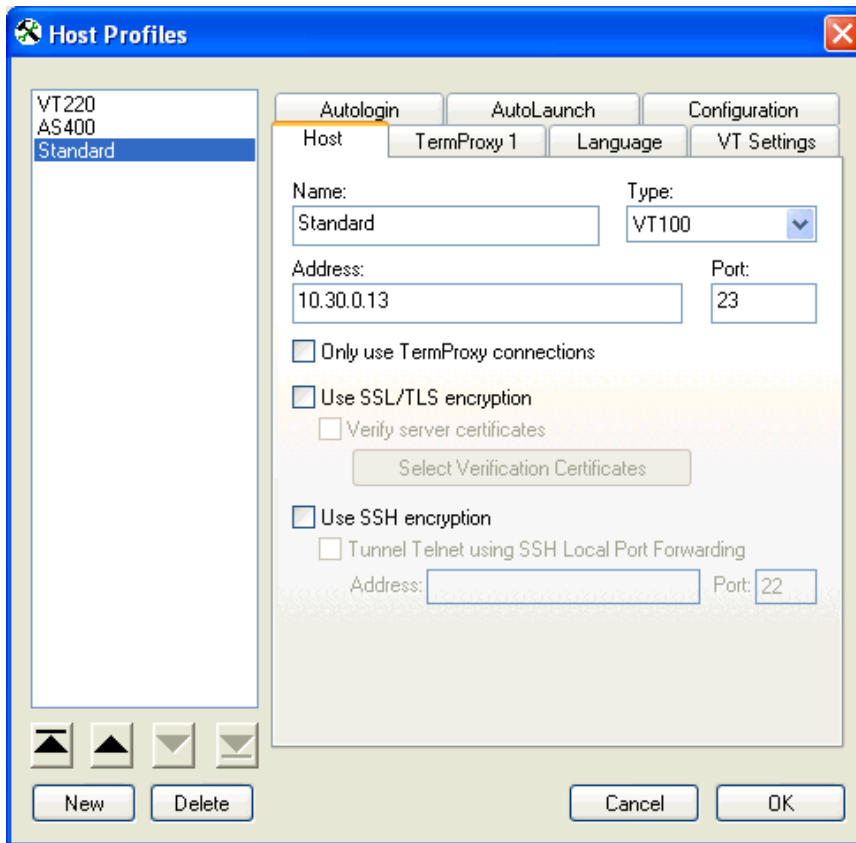
Chapter 4: Configuring the Client for ConnectPro

To configure a TE Client to use ConnectPro, modify both the Host tab and the TermProxy 1 tab in the *Host Profiles* dialog box of the Terminal Emulation configuration utility. If you are using SSL/TLS or SSH in your environment, these also must be configured in the TE Client. For information on launching the TE configuration utility, see the *Terminal Emulation Client User Guide*. The following sections provide information on how to configure the options on these tabs:

- [Host Tab](#)
- [TermProxy 1 Tab](#)
- [Using SSL/TLS with ConnectPro](#)
- [Using SSH with ConnectPro](#)

Host Tab

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



Host Profiles Dialog Box

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



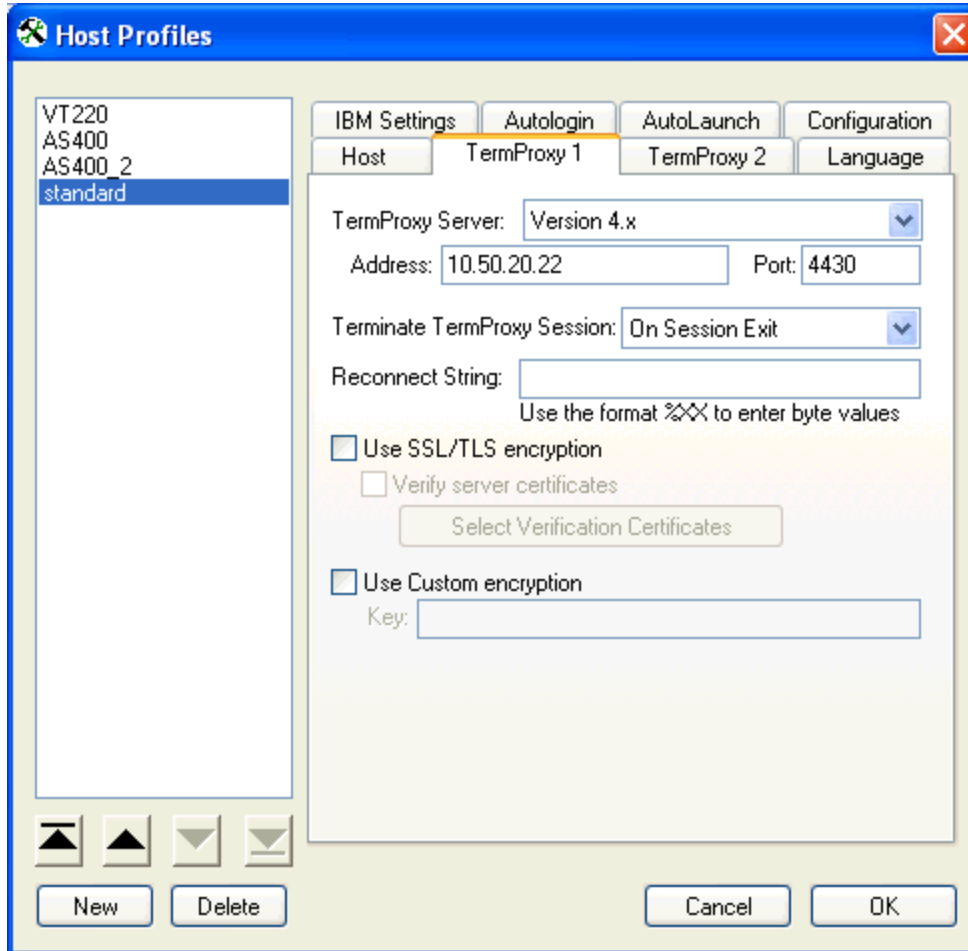
Configuration Option	Description
Name	Enter the name of the Telnet host profile.
Type	Select the type of emulation.
Address	Enter the IP address of the Telnet host.
Port	Enter the port of the Telnet host.
Only use TermProxy connections	Enable this option if you want to use ConnectPro connections only. This prevents direct connections to the target host. This option disables the Use SSL/TLS encryption option for the Telnet host, but not for ConnectPro.
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 and Use SSH encryption options will disable. For more information, see Using SSL/TLS with ConnectPro on page 29.
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.
Select Verification Certificates	This allows you to create or select verification certificates. The Verify server certificates option must be enabled for this option to be active.
Use SSH encryption	Enable this option if you want to use SSH to encrypt the data between ConnectPro and the host. If you enable this option, the Use SSL/TLS encryption option will disable.
Tunnel Telnet using SSH Local Port Forwarding	Enable this option if you want to connect to a standard Telnet by tunneling through a SSH server. This feature is optional unless you are using IBM emulation.
Address	Enter the IP address of the SSH host that will perform the tunneling.
Port	Enter the port of the SSH host that will perform the tunneling.



TermProxy 1 Tab

Once you configure the Host tab for the Client, configure the TermProxy 1 tab.

Configure up to three ConnectPro servers as failover servers. If the initial ConnectPro server cannot be reached, the client attempts to connect to subsequent ConnectPro servers before it attempts a direct connection with the 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.



TermProxy 1 Tab

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

Configuration Option	Description
TermProxy Server	The version of the ConnectPro/TermProxy server.



Configuration Option	Description
Address	Enter the IP address of the ConnectPro/TermProxy server.
Port	Enter the Port of the ConnectPro/TermProxy server.
Terminate TermProxy Session	<p>Indicates when the ConnectPro/TermProxy server should terminate the connection to the host.</p> <p>Possible Values:</p> <ul style="list-style-type: none"> • Never. The proxy server never terminates the session established with the host. The Client is responsible for terminating the session. • On Network Error. The proxy server terminates the session with the host when a network error occurs, such as a loss of network connectivity. • On Session Exit. The proxy server terminates the session with the host when the session is terminated by the Client. This is the default value. • Always. The proxy server will terminate the session with the host on a network error or when the session is terminated.
Reconnect String	<p>A reconnect string requests the last screen data that the host had before the mobile device disconnected. Input a reconnect string or use one you defined in the ConnectPro configuration file. The reconnect string in the host profile takes precedence over the reconnect string in the ConnectPro configuration file.</p> <p>Requirements for connect strings depend upon the application, but the strings are required in 5250 and 3270 environments. For more information on reconnect strings, see Configuring Reconnect Strings on page 18.</p>
Use SSL/TLS encryption	<p>Enable Use SSL/TLS encryption to encrypt data between the mobile device and the ConnectPro server.</p> <p>For more information, see Using SSL/TLS with ConnectPro on page 29.</p>
Verify server certificates	<p>Enable Verify Server Certificates to perform SSL/TLS verification between the mobile device and the ConnectPro server.</p> <p>SSL/TLS verification requires a local certificate chain (root certificate and intermediate certificates if any) on the mobile device.</p>



Configuration Option	Description
Select Verification Certificates	Once you enable the Verify Server Certificates option, the Select Verification Certificates button is active. Click this button to open the <i>Certificate Manager</i> dialog box. Then use the Certificate Manager to create, insert or remove certificates.
Use Custom encryption	Enable the Use Custom encryption option to use a custom algorithm to encrypt data between the mobile device and the ConnectPro server.
Key	Use the same key for custom encryption here that is in the ConnectPro configuration file.

Using SSL/TLS with ConnectPro

In order to use SSL or TLS with the TE Client, you will need to install a support utility on the computer from which you will deploy the Client configuration, install a support package on the device running the Client, and configure the host profile(s) for the Client. Then you will need to deploy the new Client configuration to the device.

If you plan to use verification certificates, you also need to create or import the certificates for the Client to use. If you create certificates using the TE Certificate Manager, you will need to save the certificates in the appropriate location so that the server can use them.

When you are using SSL, connect to the ConnectPro server configuration page using `https://[IP address of ConnectPro server]:[Port of ConnectPro server]`.

For information about using SSL/TLS encryption and verification with the TE Client, see the paper [Using SSL/TLS with Terminal Emulation](#) on the Wavelink Web site.

Using SSH with ConnectPro

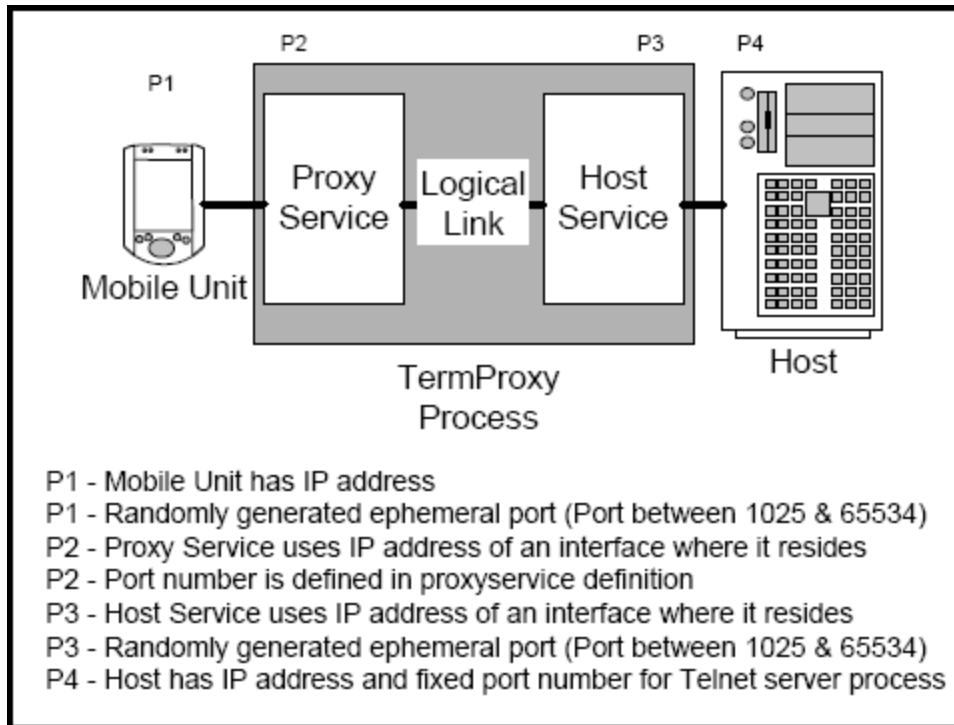
Secure Shell (SSH) is a protocol developed for transmitting private information over the Internet. The TE Client supports SSH version 1 and 2 and will automatically select the most secure protocol supported. In order to use SSH with the TE Client, you will need to install a support utility on the computer from which you will deploy the Client configuration, install a support package on the device running the Client, and configure the host profile(s) for the Client. Then you will need to deploy the new Client configuration to the device.

For more information about using SSH with the TE Client, see the paper [Using SSH with Terminal Emulation](#) on the Wavelink Web site.



Chapter 5: Using ConnectPro

The connection between the mobile device and ConnectPro is referred to as the Client-proxy connection and is handled by the proxy service. The connection between ConnectPro and the host is referred to as the proxy-host connection and is handled by the host service:



Process Overview

The ConnectPro server may reside on the same machine as the host.

Each emulation session is identified by a unique session ID when it is established through ConnectPro. This allows multiple emulation sessions on one mobile device to be established through ConnectPro.

To initiate an emulation session with ConnectPro:

- 1 Add proxy service and host service configurations using the ConnectPro web interface.
- 2 Add a host profile with information about the ConnectPro server from the TE Client configuration utility.
- 3 Connect to the host using ConnectPro.

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



- 4 View the status of your connection from the ConnectPro web interface to verify ConnectPro is being used for the session.

See the following sections for more information about using ConnectPro:

- [Restarting the ConnectPro Server](#)
- [Starting or Stopping the ConnectPro Service](#)
- [Logging and Data Capture](#)
- [Viewing ConnectPro Status and Sessions](#)
- [Managing ConnectPro HTTP Settings](#)
- [Deleting Stored Public Keys](#)

Restarting the ConnectPro Server

Restart ConnectPro from the *Restart TermProxy* page in the ConnectPro web interface immediately, or schedule an automatic restart on a daily or weekly basis.

To restart ConnectPro:

- 1 Access the ConnectPro web interface.
- 2 From the menu at the top of the page, click **Restart Server**.
The *Restart TermProxy* page appears.
- 3 Click the **Restart** button.

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

To schedule an automatic restart:

- 1 Access the ConnectPro web interface.
- 2 From the menu at the top of the page, click **Configuration**.
The *Logging and Data Capture Settings* page appears.
- 3 In the secondary navigation, click **Stored Configuration**.
The *Stored Configuration* page appears.
- 4 In the text box, modify the automatic restart section (at the end of the file by default). To modify the section, type `restart [time]`, where `[time]` is a comma-delimited list of



times that ConnectPro will automatically restart. Each time needs to follow the format HH:MM[a|p]. If there is no 'a' or 'p' following the time (representing AM or PM), the time is assumed to be in a 24-hour format. To restart only on a certain day of the week, precede the time with the day of the week.

Examples:

```
restart 10:00P
```

```
restart MONDAY22:30
```

- 5 Click **Save and Restart** to apply the new settings.

Starting or Stopping the ConnectPro Service

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

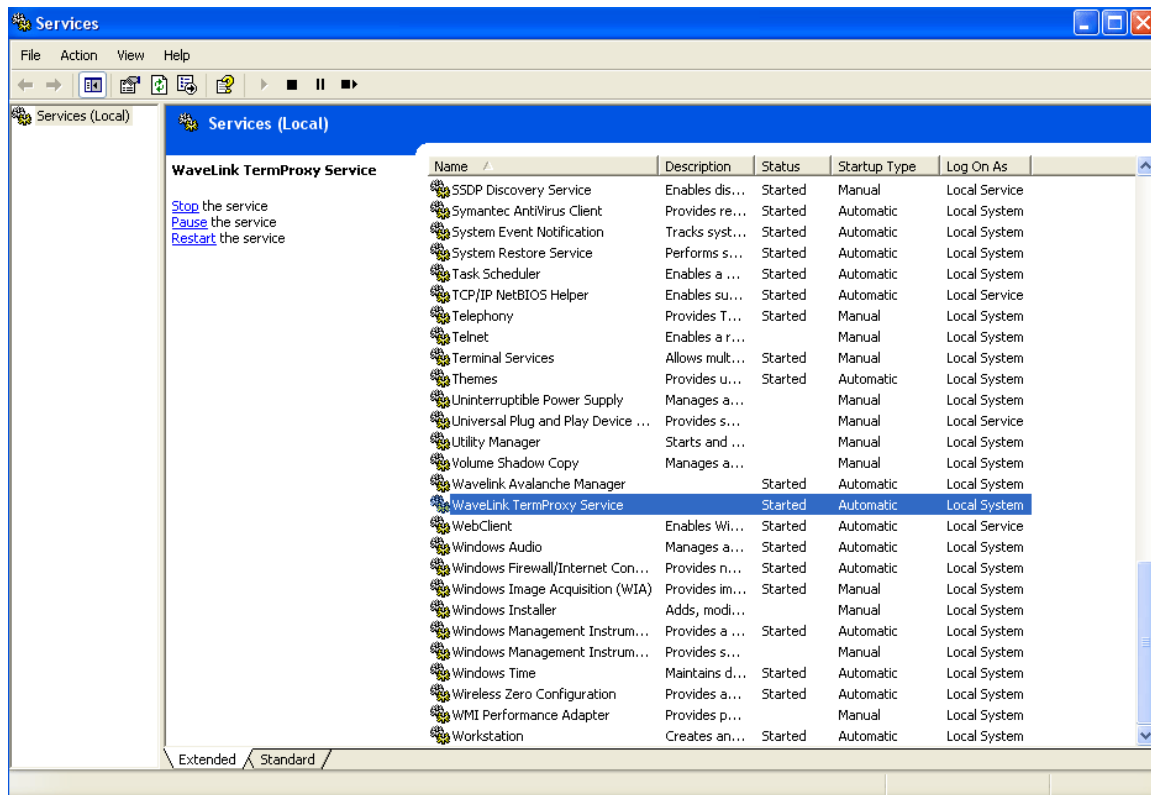
To start or stop the ConnectPro service from the Windows Services console:

- 1 Ensure that you have installed ConnectPro 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.





Services Console

- 6 Right-click the service and select **Start** or **Stop** from the context menu.

The ConnectPro service starts or stops.

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

- 1 Navigate to the directory where `wltermproxyservice.exe` is installed.
- 2 Type `wltermproxyservice -a start` to start the service, or `wltermproxyservice -a stop` to stop the service.

Logging and Data Capture

ConnectPro provides a logging service that writes information about its functions to a plain-text log file. This information allows you to evaluate errors, ConnectPro server functionality, and information about Client connection. The amount of detail that is recorded to the ConnectPro log file is configurable.

The log file is called `TermProxy.log` and is generated in the directory from which you are running the ConnectPro application. Whenever ConnectPro starts, it writes the contents of the previous `TermProxy.log` to the `TermProxy.log.bak` file and creates a new `TermProxy.log` file.



While ConnectPro is running, ConnectPro will not allow the log file to grow beyond 100 KB. Once the log file reaches 100 KB, ConnectPro 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 written to `TermProxy.log.bak` when ConnectPro is started.

This section provides the following information:

- [Setting the Logging Level](#)
- [Enabling Data Capture](#)
- [Viewing Log and Capture Files](#)

Setting the Logging Level

ConnectPro 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 the Log
Level 1	Writes only critical errors to the log file, such as errors that cause ConnectPro to fail to start.
Level 2	Writes critical errors and error messages to the log file. This includes errors that are caused by configuration and/or communication problems.
Level 3	Writes critical errors, error messages, and warnings to the log file. This includes possible operational problems.
Level 4	Writes critical errors, error messages, warnings, and informational messages to the log file. This includes information about the flow of operation.
Level 5	Writes critical errors, error messages, warnings, informational messages, and debug information to the log file. This includes information for diagnosing program malfunctions or communication problems.
Level 6	Writes critical errors, error messages, warnings, information messages, debug information and all other information to the log file. This level causes large amounts of data to be written to the log file.

By default, ConnectPro is set to logging level 4. Modify the ConnectPro logging level in the ConnectPro web interface two ways:



- In the ConnectPro stored configuration. When you modify the settings here, they are permanent.
- In the *Logging and Data Capture Settings* page. When you modify the settings here, they are temporary and will reset to the stored configuration values after a restart.

To modify the logging level in the ConnectPro configuration:

1 Access the ConnectPro web interface.

2 From the menu at the top of the page, click **Configuration**.

The *Logging and Data Capture Settings* page appears.

3 In the secondary navigation, click **Stored 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 ConnectPro.

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

1 Access the ConnectPro web interface.

2 From the menu at the top of the page, click **Configuration**.

The *Logging and Data Capture Settings* page appears.

3 Select the logging level.

4 Click **Apply Changes**.

Enabling Data Capture

Data capture records all network traffic entering and exiting the ConnectPro server. Enable data capturing from the *Logging and Data Capture Settings* page or in the ConnectPro 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 ConnectPro restart to continue capturing data.

To enable data capturing from the ConnectPro configuration:

1 Access the ConnectPro web interface.

2 From the menu at the top of the page, click **Configuration**.

The *Logging and Data Capture* page appears.

3 In the secondary navigation, click **Stored Configuration**.



- 4 In the 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 ConnectPro.

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

- 1 Access the ConnectPro web interface.

- 2 From the menu at the top of the 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 address or addresses of the Clients from which you want to capture data. If you leave the **Enter IP addresses to capture** text box empty, all Client data will be captured.

Examples of IP addresses:

Individual: 165.138.5.10

Multiple: 165.192.5.10, 10.204.140.50

Network: 165.192.5.1/24

- 5 Click **Apply Changes**.

Viewing Log and Capture Files

View the ConnectPro log file and data capture file from the web interface.

To view a ConnectPro log file:

- 1 Access the ConnectPro 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. To refresh the log file page, click **Refresh** at the top of the page.

To view the data capture file:

- 1 Access the ConnectPro 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. To refresh the data capture page, click **Refresh** at the top of the page.

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

Viewing ConnectPro Status and Sessions

This section provides information on ConnectPro proxyservice sessions. Monitor activity for each configured proxy service or suspend or resume activity.

- [Viewing Session Status](#)
- [Suspending a Session](#)
- [Viewing Session List](#)

Viewing Session Status

The ConnectPro 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.

Statistic	Description
Software Version	Displays the current version of ConnectPro
Uptime	Displays the time elapsed since ConnectPro 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 ConnectPro 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 ConnectPro was last restarted. The number in the parenthesis indicates the connections that are currently active.



Statistic	Description
Bytes Received	Total number of bytes received by both Client and host.
Bytes Sent	Total number of bytes sent from both Client and host.

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

Statistic	Description
Proxy Service Address	Displays the proxy service IP address for the specific session.
Host Service Address	Displays the host service 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 ConnectPro 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 ConnectPro was last restarted. The number in the parenthesis indicates the connections that are currently active.
Host Connection aborts	Displays the number of times the host has aborted.



Statistic	Description
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 bytes 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.

To view ConnectPro status:

- 1 Access the ConnectPro web interface.
- 2 From the menu at the top of the page, click **Current Status**.

The *Current Status* page appears.

Suspending a Session

When you suspend a ConnectPro 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 ConnectPro 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, it also displays the workstation ID of the mobile device.

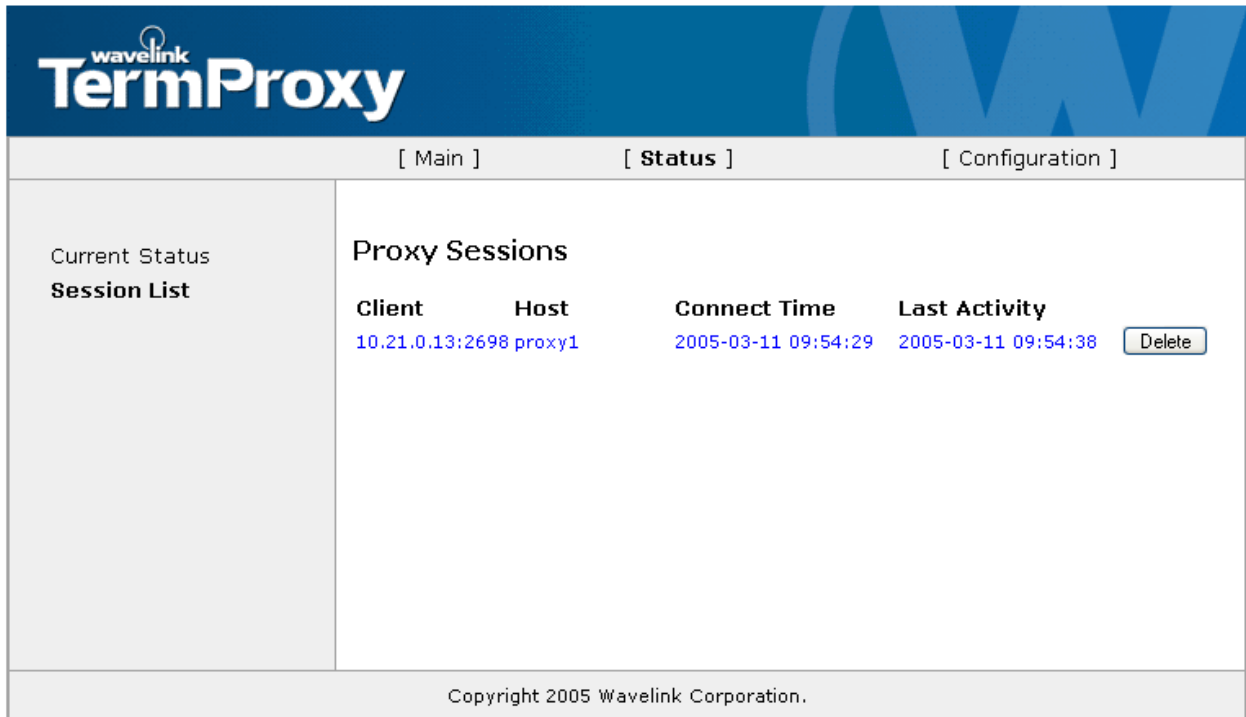
To view session list:

- 1 Access the ConnectPro web interface.
- 2 From the menu at the top of the page, click **Current Status**.

The *Current Status* page appears.

- 3 In the secondary navigation, click **Session List**.

The *Proxy Session* window appears.



The screenshot shows the Wavelink TermProxy web interface. The header is blue with the Wavelink logo and 'TermProxy' text. Below the header is a navigation bar with three tabs: [Main], [Status], and [Configuration]. The [Status] tab is selected. On the left side, there is a sidebar with 'Current Status' and 'Session List' (the latter is highlighted). The main content area is titled 'Proxy Sessions' and contains a table with the following data:

Client	Host	Connect Time	Last Activity	
10.21.0.13:2698	proxy1	2005-03-11 09:54:29	2005-03-11 09:54:38	<input type="button" value="Delete"/>

At the bottom of the page, there is a footer that reads 'Copyright 2005 Wavelink Corporation.'

Session List



Press the **Delete** button, located to the right of each session listing, to disconnect the ConnectPro sessions.

Managing ConnectPro HTTP Settings

The ConnectPro *HTTP Settings Page* allows you to manage ConnectPro web server access. Use the *HTTP Settings Page* to perform the following tasks:

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

HTTP setting changes will persist when ConnectPro is restarted. The HTTP settings are saved to the `http.cfg` file.

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

To change HTTP settings:

- 1 Access the ConnectPro 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.



	[Main]	[Status]	[Configuration]
Log Settings Proxy Configuration HTTP Settings Restart TermProxy	<h2 style="text-align: center;">HTTP Settings</h2> <p>If you have stored the HTTP settings in a file (-u@... command line option), TermProxy attempts to save your changes in that file. If your settings are not in a file, or the specified file is not writeable, any changes made here are temporary and will be discarded after a restart or shutdown.</p> <p>You need to know the administrative password to be allowed to make changes to the HTTP settings. The administrative password is different from the browser password you needed to start this session.</p> <p style="text-align: center;">Enter the administrative password, then press the VALIDATE button</p> <div style="display: flex; justify-content: space-between; align-items: flex-start;"> <div style="width: 45%;"> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="checkbox"/> Encrypt the HTTP settings file </div> <div style="width: 45%;"> <input type="button" value="Validate"/> <p>New HTTP Administrative password</p> <p>HTTP User Name</p> <p>HTTP Password</p> <p>HTTP services IP filter masks</p> </div> </div> <div style="display: flex; justify-content: space-around; margin-top: 10px;"> <input type="button" value="Save Changes"/> <input type="button" value="Reset"/> </div>		

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.

Deleting Stored Public Keys

If you change a SSH host's public keys, clear the SSH public keys that ConnectPro has saved.

To clear SSH public keys:

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

The *Logging and Data Capture Settings* page appears.

- 3 In the secondary navigation, click **SSH Settings**.

The *SSH Settings* page appears.

- 4 Click the **Clear SSH Saved Keys** button.

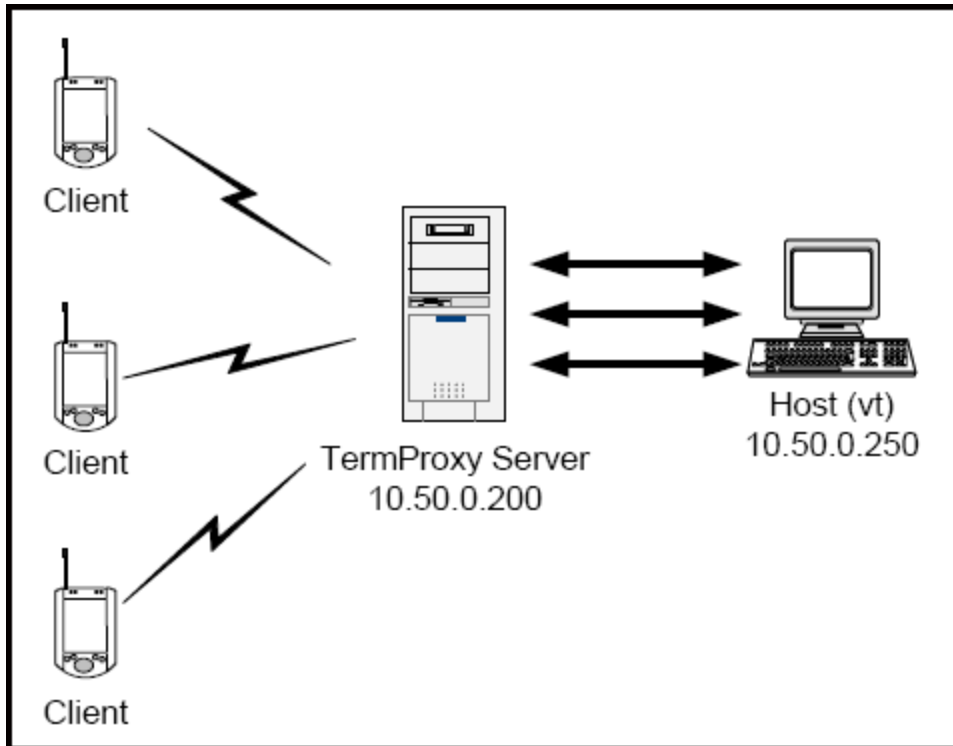


Network Scenarios

The following section contains three different ConnectPro 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 this model, clients connect to a single host through a proxy server. This example is based on VT emulation with no reconnect string.



Multiple Clients Connect to a Single Host

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

```
proxyservice proxy1
listen 10.50.0.200:4430
server VT

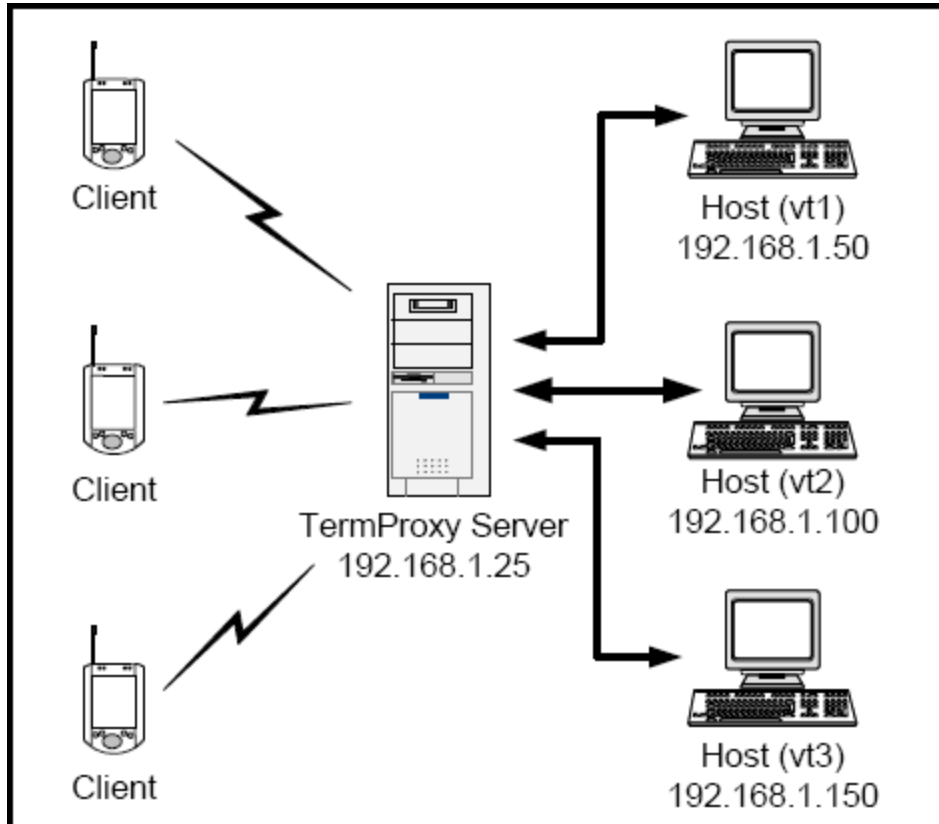
hostservice VT
connect 10.50.0.250:23
```

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 this model, 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.



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

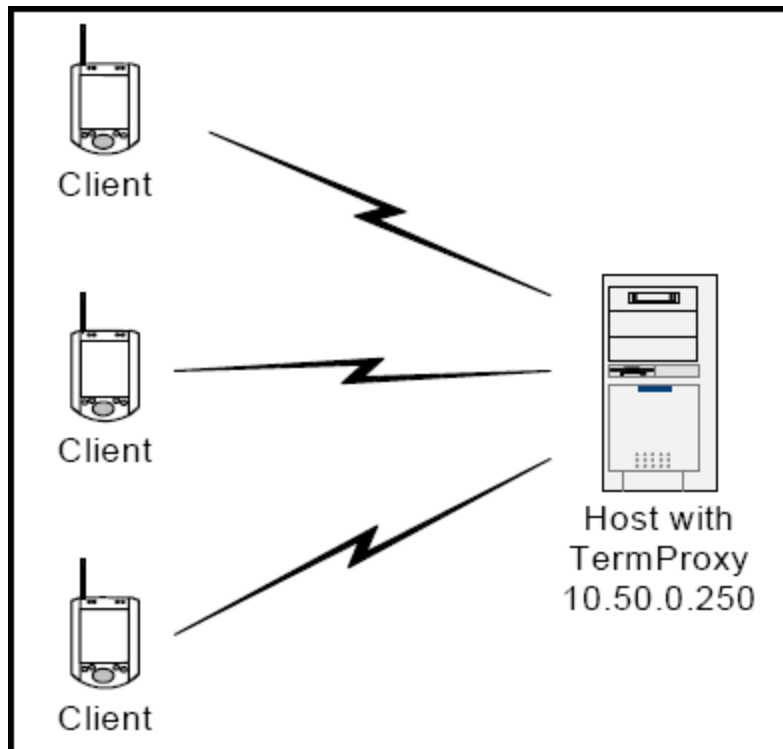
proxy //proxy entry for connection to Host 1
listen 192.168.1.25:2301
server 192.168.1.50:23
```

Add three host profiles in the TE Client. Specify the ConnectPro server in the TermProxy 1 tab of each host profile.



Scenario 3: Multiple Clients to Proxy Server/Host

In this model, several clients connect to a system that hosts the Telnet service and the ConnectPro application.



Multiple Clients Connect to a Proxy Server/Host

Configure the proxy entry in the ConnectPro 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
```

Configure the clients' host profile to direct session traffic to 10.50.0.250:4430.



ConnectPro as a Console Application

ConnectPro can be run as a console application when it is installed on a Windows system. Use command line switches to configure options, or use commands while it is running to perform actions.

Use the following switches before starting ConnectPro:

Switch	Function
<code>-c [configfile]</code>	<p>Specifies the configuration file that ConnectPro uses, where <code>[configfile]</code> is the name of the configuration file. For example: <code>[-c c:\proxy\proxy.cfg]</code>.</p> <p>Include the entire path with the file name if it is located in different directory than the default. For example: <code>[-c "c:\termproxy config\proxy.cfg"]</code>.</p> <p>By default, ConnectPro uses TermProxy.cfg within the directory where <code>wltermproxyservice.exe</code> is installed.</p>
<code>-h</code>	Displays the ConnectPro help, which lists the available switches.
<code>-k [configfile]</code>	<p>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 <code>wltermproxyservice.exe</code> resides. For example: <code>[-k c:\secure\skey.pem]</code></p>
<code>-l [level]</code>	<p>Sets the ConnectPro logging level. The <code>[loglevel]</code> parameter is the logging level to which you want to set ConnectPro. <code>[loglevel]</code> 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 Setting the Logging Level on page 34.</p>
<code>-s [certfile]</code>	<p>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 <code>wltermproxyservice.exe</code> resides. For example: <code>[-s c:\secure\scert.pem]</code></p>
<code>-u [httpacct]</code>	<p>Indicates the ConnectPro web server account user name and password on the command line. Example: <code>[-u <userid>:<password>]</code></p>



Switch	Function
	Indicates a reference file that contains this information such as <code>http.cfg</code> . For example: <code>[-u @http.cfg]</code> or <code>[-u @c:\proxy\http.cfg]</code>
<code>-v</code>	Displays the ConnectPro version information.

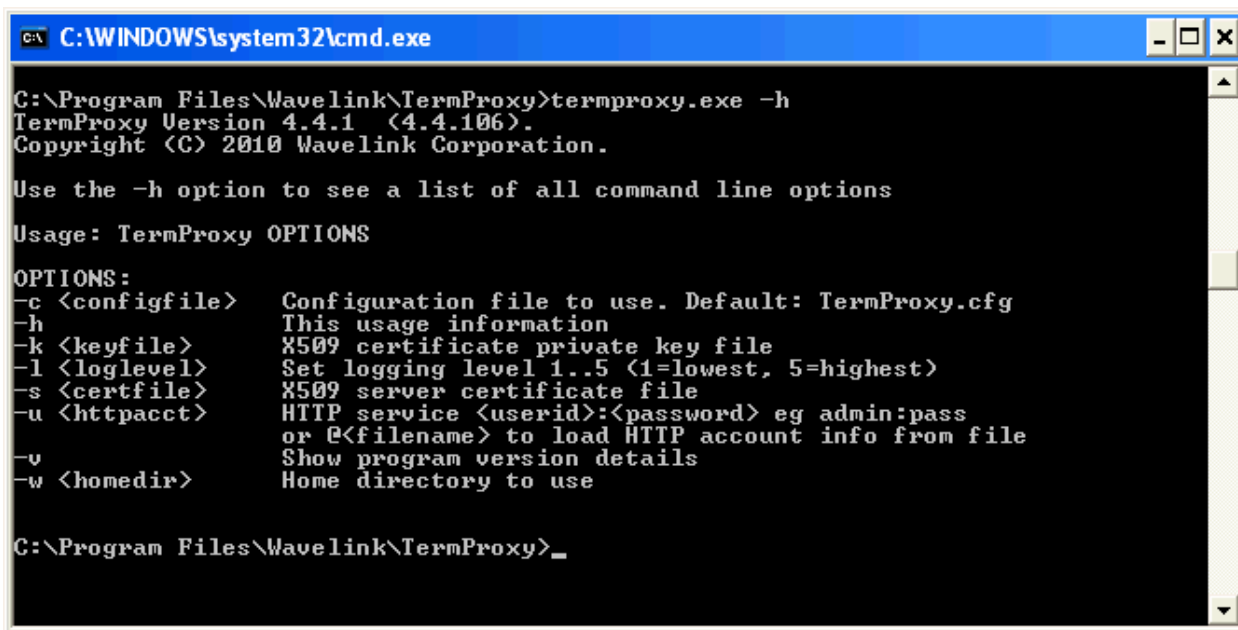
Use the following commands while ConnectPro is running as a console application:

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

To run ConnectPro from the command line:

- 1 From a command line, navigate to the directory that contains `TermProxy.exe`.
 - To use command line switches, type `termproxy.exe [switch]`, where `[switch]` is the switch that you want to use.





```
C:\WINDOWS\system32\cmd.exe

C:\Program Files\Wavelink\TermProxy>termproxy.exe -h
TermProxy Version 4.4.1 (4.4.106).
Copyright (C) 2010 Wavelink Corporation.

Use the -h option to see a list of all command line options

Usage: TermProxy OPTIONS

OPTIONS:
-c <configfile> Configuration file to use. Default: TermProxy.cfg
-h             This usage information
-k <keyfile>   X509 certificate private key file
-l <loglevel>  Set logging level 1..5 (1=lowest, 5=highest)
-s <certfile> X509 server certificate file
-u <httpacct> HTTP service <userid>:<password> eg admin:pass
              or @<filename> to load HTTP account info from file
-v           Show program version details
-w <homedir> Home directory to use

C:\Program Files\Wavelink\TermProxy>_
```

ConnectPro switch

- To start ConnectPro, type `termproxy.exe`.

ConnectPro runs with the desired options. Use the commands in the table above to restart, exit, change the log levels or data capture, or dump the current session states to the log file.



Wavelink Contact Information

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

E-mail Wavelink Customer Support at: CustomerService@wavelink.com

For customers within North America and Canada, call the Wavelink Technical Support line at 801-316-9000 (option 2) or 888-699-9283.

For international customers, call the international Wavelink Technical Support line at +800 9283 5465.

For Europe, Middle East, and Africa, hours are 9 AM - 5 PM GMT.

For all other customers, hours are 7 AM - 7 PM MST.

