



**Wavelink Telnet Client  
User Guide**

tn-ug-20070821

*Revised 08/21/07*

Copyright © 2007 by Wavelink Corporation All rights reserved.

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

Email: [sales@wavelink.com](mailto: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

<b>Chapter 1: Introduction</b>	<b>9</b>
Document Assumptions .....	9
Document Conventions .....	9
About the Telnet Client .....	10
Telnet Client Overview .....	10
Deployment Methods .....	11
Telnet Client Components .....	11
About Host Profiles .....	12
About Emulation Parameters .....	12
About Localization .....	12
About SSL .....	12
About Scripting .....	12
About Keyboard Creator .....	13
Telnet Client Functionality .....	13
Voice-Enabled Emulation .....	13
Telnet Client Version and Supported Features Matrix .....	14
<b>Chapter 2: Installation and Configuration</b>	<b>17</b>
Installing the Telnet Client .....	17
Cold Boot Recovery .....	18
Configuring the Telnet Client .....	18
Configuration Overview .....	18
Configuration Support Matrix .....	20
Using Avalanche Manager to Configure the Telnet Client .....	21
Using Microsoft ActiveSync to Configure the Telnet Client .....	23
Deploying Configurations .....	24
Deploying Configurations via Avalanche Manager .....	24
Preparing for Updates .....	24
Preparing for Serial Updates .....	25
Preparing for RAPI Updates .....	26
Preparing for IP Updates .....	27
Downloading the Configuration to the Mobile Device .....	29
Deploying Configurations via Microsoft ActiveSync .....	30
<b>Chapter 3: Host Profiles</b>	<b>31</b>
Overview of Host Profiles .....	31
Configuring a Host Profile .....	33
Adding a Host Profile .....	34
Modifying an Existing Host Profile .....	35
Deleting a Host Profile .....	36
Subnet-Specific Addresses .....	37
Host Profiles and SSL .....	38
Installing the SSL Support Package on the Host System .....	38

Installing the SSL Support Package on the Mobile Device . . . . .	39
Enabling SSL . . . . .	39
Enabling Certificate Verification . . . . .	41
Host Profiles and Wavelink TermProxy. . . . .	44
Configuring a TermProxy-Only Connection . . . . .	44
Configuring TermProxy Failover . . . . .	46
Host Profile Settings . . . . .	48
Host Settings . . . . .	48
TermProxy Settings . . . . .	51
IBM Settings . . . . .	53
VT Settings . . . . .	55
WEB Settings . . . . .	57
Autologin Settings . . . . .	57
AutoLaunch Settings . . . . .	60
Configuration Settings . . . . .	61
<b>Chapter 4: Emulation Parameters</b> . . . . .	<b>63</b>
About Emulation Parameters. . . . .	63
About Per-Host Emulation Parameters . . . . .	63
About Global Emulation Parameters . . . . .	64
Configuring Emulation Parameters . . . . .	64
Overview of Configuring Emulation Parameters . . . . .	64
Accessing Global Emulation Parameters . . . . .	64
Using Microsoft ActiveSync . . . . .	65
Using Avalanche Manager . . . . .	67
Accessing Per-Host Emulation Parameters . . . . .	69
Using Microsoft ActiveSync . . . . .	69
Using Avalanche Manager . . . . .	71
Using Configuration Manager. . . . .	72
Modifying Emulation Parameters . . . . .	74
Using the Find Function . . . . .	75
Switching to Alphabetized View . . . . .	76
<b>Chapter 5: Scripting</b> . . . . .	<b>79</b>
Overview of Scripting . . . . .	79
Launching the Script Editor . . . . .	80
Creating Scripts Using the Script Editor. . . . .	82
Configuring the Script Name . . . . .	83
Selecting the Activation Method . . . . .	83
Select from Menu . . . . .	84
On Key Combination . . . . .	84
When Session Connects . . . . .	85
On Barcode, MSR or RFID Scan . . . . .	86
On Screen Update . . . . .	87
Creating the Script Code . . . . .	88
Creating Variables . . . . .	88

---

Selecting Host Profiles .....	90
Performing Script Capturing .....	92
Field Data ID Button .....	96
Editing Scripts .....	96
Importing Scripts .....	97
Saving and Exporting Scripts .....	98
Deploying Scripts .....	100
Executing Scripts .....	100
Select from Menu .....	100
On Key Combination .....	101
When Session Connects .....	101
On Barcode, MSR, or RFID Scan .....	102
On Screen Update .....	102
<b>Chapter 6: Keyboard Creator</b> .....	<b>103</b>
Overview of Keyboard Creator .....	103
Launching the Keyboard Creator .....	103
Selecting Keyboard Files .....	105
Creating Keyboards .....	106
Adding a new keyboard .....	106
Sizing Keyboards .....	108
Deleting Keyboards .....	108
Importing Keyboard Graphics .....	109
Creating and Configuring Keys .....	109
Adding a new key .....	110
Sizing and Positioning Keys and Rows .....	112
Deleting Keys .....	113
Deploying the Keyboard to the Telnet CE Client .....	113
<b>Chapter 7: Resource Editor</b> .....	<b>115</b>
Overview of Resource Editor .....	115
Launching the Resource Editor .....	115
Using the Resource Editor .....	116
Adding a Bitmap .....	116
Adding a Sound .....	117
Playing Sounds .....	117
Editing Files .....	117
Deploying Files to the Telnet Client .....	119
<b>Chapter 8: Licensing</b> .....	<b>121</b>
Overview of Licensing .....	121
Authorization Methods .....	122
Types of Licenses .....	123
About Platform Licenses .....	123
About Maintenance Licenses .....	123
Licensing Methods .....	123

Manually Licensing the Telnet Client .....	124
Using License Server to License the Telnet Client .....	125
Using a Local License Server .....	125
Using a Remote or Specific License Server .....	126
Using the Demo License .....	127

## **Chapter 9: Using the Telnet Client** **129**

Using the Telnet Client and Connecting to Hosts .....	129
Launching the Telnet Client .....	129
Launching the Telnet Client From Windows .....	130
Launching the Telnet Client from Avalanche .....	131
Initiating a Telnet Session .....	133
Disconnecting a Telnet Session .....	135
Exiting the Telnet Client .....	136
Working with Multiple Concurrent Telnet Sessions .....	137
Overview of Multiple Concurrent Sessions .....	137
Initiating an Additional Telnet Session .....	137
Switching Between Active Telnet Sessions .....	139
Disconnecting a Session .....	140
Using the Standard Virtual Emulation Keyboard .....	141
Using the Basic Virtual Emulation Keyboard .....	142
Using the 5250/3270 Virtual Emulation Keyboard .....	143
Using the VT/HP Virtual Emulation Keyboard .....	145
Using the WEB Virtual Emulation Keyboard .....	147
Using Screen Panning .....	149
Using ActiveText .....	149
Simple Number Menu Item .....	150
AS/400-Style Function Key .....	150
Using the Telnet Client Diagnostics Utility .....	151
Accessing the Telnet Client Diagnostics Utility .....	151
Performing a Keyboard Test .....	152
Performing a Scan Test .....	154
Performing a Windows Keyboard Test .....	155
Using the Telnet Client Options Menu .....	156

## **Chapter 10: Industrial Browser (WEB Emulation)** **159**

Overview of the Industrial Browser .....	159
Licensing .....	159
Industrial Browser Host Profile Settings .....	160
HTTP Proxy Tab .....	160
HTTPS Proxy Tab .....	161
Access List Tab .....	163
Configuration Tab .....	164
Using the Industrial Browser .....	165
Basic Navigation .....	166
Specifying the Home Page .....	166

Developing Web Pages for the Industrial Browser. ....	167
META Tags .....	167
BatteryNavigate .....	168
OnAllKeys, OnKey..., OnKey0x... .....	169
OnStartup, IDA .....	169
PowerOn .....	169
Printing .....	169
Scanner .....	171
ScannerNavigate, ScannerProcessed .....	171
SignalNavigate .....	172
SpeechFromText .....	172
SpeechSetting .....	172
TextFromSpeech .....	172
Symbolologies .....	173
Element-Specific Actions .....	173
IDA Commands .....	175
IDA_COLDBOOT .....	177
IDA_COLDBOOT_PROMPT .....	178
IDA_KEYBOARD_WEB, IDA_KEYBOARD_SHOW, or IDA_KEYBOARD_UP .....	178
IDA_KEYBOARD_NUM or IDA_KEYBOARD_NUMERIC ...	178
IDA_KEYBOARD_NONE, IDA_KEYBOARD_HIDE, or IDA_KEYBOARD_DOWN .....	178
IDA_PROGRAM_EXIT .....	178
IDA_PROGRAM_EXIT_PROMPT .....	178
IDA_REPRINT .....	178
IDA_SESSION_S1, IDA_SESSION_S2, IDA_SESSION_S3, IDA_SESSION_S4 178	
IDA_SCAN_DISABLE or IDA_SCAN_SUSPEND .....	178
IDA_SCAN_ENABLE or IDA_SCAN_RESUME .....	178
IDA_SCAN_FORWARD .....	179
IDA_SESSION_DISCONNECT .....	179
IDA_SESSION_DISCONNECT_PROMPT .....	179
IDA_SESSION_NEXT .....	179
IDA_SESSION_PREVIOUS .....	179
IDA_SIP_SHOW or IDA_SIP_UP .....	179
IDA_SIP_HIDE or IDA_SIP_DOWN .....	179
IDA_SIP_TOGGLE or IDA_SIP_TOGGLEHIDE .....	179
IDA_SUSPEND or IDA_SUSPEND_DEVICE .....	179
IDA_SUSPEND_PROMPT .....	180
IDA_URL_BACK or IDA_BACK .....	180
IDA_URL_BACK_DISABLE or IDA_BACK_DISABLE .....	180
IDA_URL_BACK_ENABLE or IDA_BACK_ENABLE .....	180
IDA_URL_FORWARD or IDA_FORWARD .....	180
IDA_URL_FORWARD_DISABLE or IDA_FORWARD_DISABLE .....	180
IDA_URL_FORWARD_ENABLE or IDA_FORWARD_ENABLE .....	180

IDA_URL_HOME or IDA_HOME	181
IDA_URL_HOME_DISABLE or IDA_HOME_DISABLE	181
IDA_URL_HOME_ENABLE or IDA_HOME_ENABLE	181
IDA_URL_REFRESH or IDA_REFRESH	181
IDA_URL_STOP or IDA_STOP	181
IDA_WARMBOOT	181
IDA_WARMBOOT_PROMPT	181
IDA_ZOOM_DISABLE or IDA_FONT_DISABLE	181
IDA_ZOOM_ENABLE or IDA_FONT_ENABLE	182
IDA_ZOOM_LARGER or IDA_FONT_LARGER	182
IDA_ZOOM_LARGEST or IDA_FONT_LARGEST	182
IDA_ZOOM_MEDIUM or IDA_FONT_MEDIUM	182
IDA_ZOOM_MINUS or IDA_FONT_MINUS	182
IDA_ZOOM_PLUS or IDA_FONT_PLUS	183
IDA_ZOOM_SMALLER or IDA_FONT_SMALLER	183
IDA_ZOOM_SMALLEST or IDA_FONT_SMALLEST	183

## **Chapter 11: Avalanche Integration** **185**

Overview of Avalanche Integration	185
Using Session Monitor	186
Enabling Session Monitor	186
Configuring Session Monitor	186
Launching Session Monitor	188
Session Override	189
Tracing Sessions	190
Using Real-Time Statistics	191
Viewing Real-Time Statistics	192
Modifying Real-Time Statistics	195

## **Chapter 12: Manually Configuring the Telnet Client** **197**

Manually Configuring Host Profiles	197
Accessing Host Profiles	197
Creating a New Host Profile	198
Modifying an Existing Host Profile	199
Deleting an Existing Host Profile	200
Host Profile Settings	201
Edit Host Profile Parameters	201
More 5250 Options	202
More VT Options	203
Edit AutoLogin	204
Manually Configuring Emulation Parameters	205
Accessing and Modifying Per-Host Emulation Parameters	206
Per-Host Emulation Parameters	207
VTXX Settings	207
IBM Host Settings	208
WEB Settings	209



---

Message Settings .....	211
Font Settings .....	213
Display Settings .....	215
View Settings .....	216
Cursor Settings .....	218
Beeps Settings .....	220
Telnet Settings .....	220
Printer Settings .....	221
<b>Appendix A: Using Microsoft ActiveSync</b> .....	<b>225</b>
Requirements .....	225
Overview of Creating a Partnership .....	225
Selecting the Microsoft ActiveSync Connection Method on the Mobile Device .....	225
Selecting the Microsoft ActiveSync Method on the Host System .....	226
Freeing a COM Port .....	229
Creating a Partnership .....	229
Creating a Standard Partnership .....	230
Creating a Guest Partnership .....	234
<b>Appendix B: Common Configuration Tasks</b> .....	<b>239</b>
Configuring Passwords .....	239
Configuring the Number of Concurrent Sessions .....	241
Configuring IP Printing .....	242
Configuring License Server IP Address .....	243
Configuring Telnet Client Display Settings .....	244
Configuring Telnet Client Lockdown .....	245
Configuring Key Macros .....	247
Configuring Screen Panning .....	248
Configuring ActiveText .....	250
Configuring Scan Handlers .....	251
Configuring Autologin for VT Emulation .....	253
Configuring Telnet Negotiation Strings for VT Emulation .....	254
Configuring Workstation IDs for 5250/3270 Emulation .....	256
Enabling Battery Strength and Signal Strength Icons .....	257
Configuring Indicator Settings .....	259
<b>Appendix C: Using the Telnet Client License Server</b> .....	<b>261</b>
Telnet Client License Server Overview .....	261
License Server Versions and Maintenance Licenses .....	262
Installing the Telnet Client License Server .....	263
Installation Methods .....	263
Installing the License Server as a Windows Application .....	263
Installation Requirements .....	264
Installing the License Server .....	264
Installing License Server as a Windows Service .....	265
Using the License Server .....	265

Launching the License Server .....	265
Adding a License .....	266
Releasing a License .....	268
Viewing License Information .....	268
Removing a License .....	269
Changing License Server Settings .....	269
<b>Appendix D: Wavelink Contact Information</b>	<b>271</b>
<b>Glossary</b>	<b>273</b>
<b>Index</b>	<b>281</b>

# Chapter 1: Introduction

This document provides information about installing, configuring, and using the Wavelink Telnet Client for Windows CE-based mobile devices.

This section provides the following information:

- Document Assumptions
- Document Conventions
- About the Telnet Client
- Telnet Client Version and Supported Features Matrix

## Document Assumptions

This document assumes that the reader has the following:

- Familiarity with Windows CE operating systems and the mobile device to which you are deploying the Wavelink Telnet Client.
- Knowledge of wireless networks and wireless networking protocols (IEEE 802.11b).
- Knowledge of TCP/IP, including IP addressing, subnet masks, routing, BOOTP/DHCP, WINS, and DNS.
- Knowledge of Telnet services and terminal emulation, including IBM 5250/3270, HP, and VT100/220.
- Knowledge of Wavelink Avalanche Manager and Avalanche Enablers (optional, for users that intend to install and configure the Telnet Client via Avalanche Manager).

## Document Conventions

The following section contains information about text-formatting conventions in this manual.

Table 1-1 lists the conventions that are used in this manual.

Convention	Description
courier new	<p>Any time you interact directly with text-based user interface options, such as a button, or type specific information into a text box, such as a file pathname, that option appears in the <i>Courier New</i> text style. This text style is also used for keys that you press, filenames, directory locations, and status information.</p> <p>For example:</p> <p>Press <code>ENTER</code>.</p> <p>Click <code>OK</code>.</p>
<b>bold</b>	<p>Any time this document refers to a labelled user interface option, such as descriptions of the choices in a dialog box, that option appears in the <b>Bold</b> text style.</p> <p>Examples:</p> <p>Enable the <b>DHCP</b> checkbox.</p> <p>Access the Telnet Client <b>Session</b> menu.</p>
<i>italics</i>	<p>Italicized text is used to indicate the name of a window or dialog box.</p> <p>For example:</p> <p>The <i>Update Utility</i> dialog box.</p> <p>The <i>Profile Manager</i> dialog box.</p>

**Table 1-1:** Text-Formatting Conventions

If you have questions about the terminology in this document, see the *Glossary* on page 269.

## About the Telnet Client

This section provides an overview of the Telnet Client.

### Telnet Client Overview

The Telnet Client is a Windows-based application that facilitates IBM 5250/3270, VT 100/220, HP Telnet, and WEB emulation.

## Deployment Methods

Currently, you can use one of the following methods to install and configure the Telnet Client on a mobile device:

- **Microsoft ActiveSync.** You can install the Telnet Client configuration utility on a host PC. The configuration utility uses an ActiveSync connection between the host PC and the mobile device to deploy the Telnet Client and Telnet Client configurations to the mobile device.
- **Wavelink Avalanche Manager.** If your mobile device is running the Avalanche Enabler, you can use Avalanche Manager to deploy the Telnet Client and Telnet Client configurations to a mobile device.
- **Third-Party Applications.** Wavelink supports some third-party deployment applications. For more information about supported deployments for your device, please see the Telnet Client installation guide for your mobile device.

## Telnet Client Components

The Telnet Client has a number of configurable components, including:

- Host profiles
- Emulation parameters
- Localization
- SSL settings
- Scripts
- Virtual keyboards

---

**NOTE** Scripts and virtual keyboard settings may only be deployed to mobile devices via Avalanche Manager. If you are using Microsoft ActiveSync or a third-party application to deploy the Telnet Client and Telnet Client configurations to your mobile devices, you will need to manually transfer the script files and virtual keyboard files to each mobile device.

---

### **About Host Profiles**

A host profile contains all of the information that a mobile device needs to connect to a particular host, including the IP address of the host, the TCP port number on which the host is listening for Telnet requests, the emulation type, and login information.

Host profiles provide an easy way for users at a mobile device to establish a connection with a host without having to remember the parameters that are required to establish the session.

### **About Emulation Parameters**

The configuration utility allows you to configure the emulation parameters for Telnet sessions. For example, you can change the way the virtual screen displays on the mobile device, the type and size of font that is used, and the type of printer to which the mobile device may be connected.

You can configure global and per-host emulation parameters.

Global emulation parameters apply to terminal emulation with hosts for which you have not configured a per-host profile.

Configuring per-host emulation parameters allows you to specify the emulation parameters for terminal emulation sessions with a particular host.

### **About Localization**

Localization allows you to deploy language profiles with the Telnet Client. The language profile allows you to convert common textual strings into a different language. The Telnet Client will then display the converted string rather than the native string.

### **About SSL**

The Telnet Client allows SSL-encrypted Telnet connections between a mobile device and a host system. The Telnet Client also provides certificate verification for SSL connections. You may import your own trusted certificates into the Telnet Client, or you may use the Telnet Client installation and configuration utility to create your own certificates, which you can then import to your Telnet server or Wavelink TermProxy server.

### **About Scripting**

The Telnet Client provides automated services through scripting. For example, you might create a user-login script. Telnet Client scripting provides for the automatic generation of scripts through script recording.

Alternatively, use the Script Editor to create your own scripts or to modify recorded scripts.

### **About Keyboard Creator**

Use the Telnet Client Keyboard Creator to modify the standard Telnet Client virtual keyboards to meet the needs of your production environment. The Keyboard Creator allows you to completely modify the layout of the virtual keyboard for each emulation type. Additionally, import your own graphic files (bitmaps) to create your own unique buttons for the keyboard.

### **Telnet Client Functionality**

The Telnet Client provides the following functionality:

- Use host profiles to initiate Telnet sessions with hosts.
- Connect to a host through Wavelink TermProxy.
- Engage in up to four simultaneous Telnet sessions.
- Configure Wavelink licensing.
- Configure new host profiles.
- View and modify certain per-host emulation parameters, including scan codes and symbologies.
- View the current device wireless and IP settings.
- View Telnet Client version information.
- Integration with the Avalanche framework to provide session monitoring and viewing of real-time statistics from Avalanche Management Console.
- Use WEB Emulation to connect to web pages with your mobile device.

### **Voice-Enabled Emulation**

Telnet Client version 7.0 supports Voice-Enabled Emulation, which is available in separate Avalanche packages. Voice-Enabled Emulation is a verbal communication system that facilitates real-time voice communication between a host computer and a mobile device user. For more information, refer to *Wavelink Telnet Client Voice-Enabled Emulation Reference Guide*.

---

**NOTE** To obtain Voice-Enabled Emulation packages, please contact Wavelink Customer Service. *Appendix D: Wavelink Contact Information* on page 271 provides Wavelink contact information.

---

## Telnet Client Version and Supported Features Matrix

The key features of the Telnet Client - host profiles, emulation parameters, localization, SSL support, scripting, keyboard building, and Avalanche integration - may not be supported in your version of the Telnet Client.

The following table provides information about the supported features in each major revision of the Telnet Client.

Telnet Client Version	Host Profiles	Emulation Parameters	Local-ization	SSL Support	Scripting	Key-board Builder	Avalanche Integration	Industrial Browser	Voice-Enabled Emulation
4.xx-xx	Yes	Yes	Yes	No	No	No	No	No	No
5.00-xx	Yes	Yes	Yes	Yes	No	No	Yes	No	No
5.1-xx	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
6.0-xx	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
7.0-xx	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

**Table 1-2:** *Telnet Client Version and Supported Features Matrix*

The Telnet Client version number consists of three numbers:

- A version number
- A revision number
- A build number

For example, if your version number is 5.00-10, then:

- 5 is the version number



- 00 is the revision number
- 10 is the build number



## Chapter 2: Installation and Configuration

This section provides the following information:

- Installing the Telnet Client
- Configuring the Telnet Client
- Deploying Configurations

### Installing the Telnet Client

This section provides an overview of the Telnet Client.

Currently, you can use one of the following methods to install the Telnet Client on a mobile device:

- **Microsoft ActiveSync.** You can install the Telnet Client configuration utility on a host PC. The configuration utility uses an ActiveSync connection between the host PC and the mobile device to deploy the Telnet Client and Telnet Client configurations to the mobile device.
- **Wavelink Avalanche Manager.** If your mobile device is running the Avalanche Enabler, you can use Avalanche Manager to deploy the Telnet Client and Telnet Client configurations to a mobile device.
- **Third-Party Applications.** Wavelink supports some third-party deployment applications. For more information about supported deployments for your device, please see the Telnet Client reference guide for your mobile device.

Because installation methods vary across mobile devices, each mobile device has its own reference guide. For information about installing the Telnet Client on your mobile device, please see the reference guide for that mobile device.

---

**NOTE** To obtain the reference guide for your mobile device, please contact Wavelink customer service. *Appendix D: Wavelink Contact Information* on page 267 contains Wavelink contact information.

---

## **Cold Boot Recovery**

All Telnet Client installations are designed to survive a device cold boot. Additionally, the Telnet Client is configured to automatically re-install in the event of a cold boot. The cold boot recovery process ensures that not only the Telnet Client application survives a cold boot, but also the Telnet Client configuration. Any deviation or exception to this process will be noted in the reference guide for your mobile device.

To allow the Telnet Client to survive a cold boot, a backup copy of the Telnet Client is stored in the non-volatile (Flash) memory of the device. A copy of any configuration files for the Telnet Client are also stored in this location when they are downloaded to the mobile device.

Cold boot recovery processes vary across mobile devices. Each Telnet Client is designed to use the recovery method of the mobile device for which it has been designed.

## **Configuring the Telnet Client**

This section provides the following information:

- Configuration Overview
- Configuration Support Matrix
- Using Microsoft ActiveSync to Configure the Telnet Client
- Using Avalanche Manager to Configure the Telnet Client

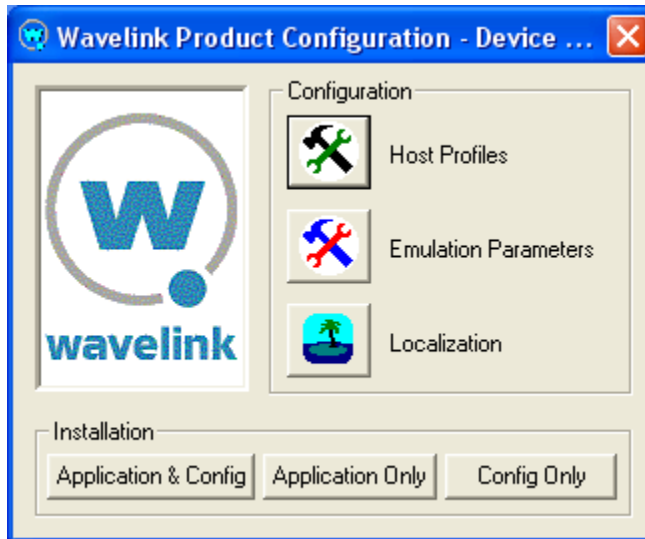
### **Configuration Overview**

Under most circumstances, you will use the same installation/configuration application to configure the Telnet Client that you used to deploy the Telnet Client to your mobile device.

The following tasks describe the process of configuring the Telnet Client:

- 1 Use the installation and configuration application to create and store Telnet Client configuration files on the host system.
- 2 Use the installation and configuration application to download the configuration files to the mobile device.

For example, if you installed the Telnet Client to a mobile device using the Microsoft ActiveSync installation and configuration utility, then you would also use the same utility to create the Telnet Client configuration files. After creating and saving the configuration files on the host system, you would then use the installation and configuration utility to push the configuration files down to the mobile device over an ActiveSync connection between the host system and the mobile device.



**Figure 2-1.** ActiveSync Installation and Configuration Utility

You may configure the following parameters and options for the Telnet Client:

- **Host Profiles.** A host profile contains all of the required information for a mobile device to connect to a host system, including an alias, IP address, TCP port, and other emulation-specific parameters. The Telnet Client supports multiple host profiles to allow a user at the device to easily create a Telnet session with a host system.
- **Emulation Parameters.** Emulation parameters provide control over many aspects of an emulation session, including key macros, text and screen display, and barcode scanning. You may control the settings of an emulation session on a global level or on a per-host level.

- **Localization.** Localization allows you to convert strings of text from one language to another. Use the Localization tool to create conversions, then configure the Telnet Client to use the appropriate language. For example, you might create support files to convert server strings from English to Spanish.
- **SSL and SSL Certificates.** Some versions of the Telnet Client support encryption-protected Telnet connections via SSL. You may also configure the Telnet Client for SSL certificate validation. SSL is configured via host profiles. You may also use the configuration and installation utility to import certificates from trusted servers or to generate new certificates that you can then export to your Telnet or Wavelink TermProxy server(s).
- **Scripting.** Scripting allows you to automate functions within the Telnet Client. For example, you might create a login script for users. You may record scripts, or you may use the Script Editor to create new scripts or modify existing scripts.
- **Keyboard Builder.** Use the Keyboard Builder to generate virtual keyboards for your Telnet Client. You may create any number of virtual keyboards to meet the needs of your production environment.
- **Resource Editor.** The Resource Editor allows you to import graphic and sound files that can be deployed to your mobile devices. You may add, modify and deploy any .bmp or .wav file using the Resource Editor.

## Configuration Support Matrix

Depending on the Telnet Client installation and configuration utility that you are using, the applications and tools that allow you to configure Telnet Client features may not be available. Table 2-1 provides information about the configuration tools that are available for your chosen installation and configuration method:

Deployment Method	Host Profiles	Emulation Parameters	Localization	SSL Support	Scripting*	Keyboard Builder
Avalanche	Yes	Yes	Yes	Yes	Yes	Yes
ActiveSync	Yes	Yes	Yes	Yes	No	No
Third-Party Application	Yes	Yes	Yes	Yes	No	No
* You may configure scripting through the Telnet Client interface on the mobile device						

**Table 2-1:** Telnet Client Configuration Support Matrix

## Using Avalanche Manager to Configure the Telnet Client

You may use the Avalanche framework to update the Telnet Client configuration.

### To configure the Telnet Client through Avalanche Manager:

- 1 Ensure that the Telnet Client Avalanche package is installed in Avalanche Manager.

---

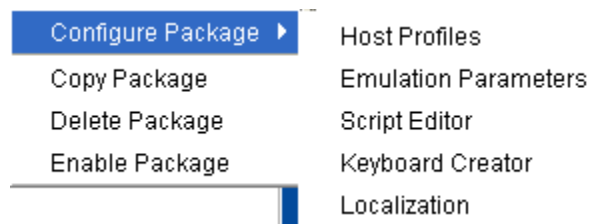
**NOTE** For more information about installing the Telnet Client in Avalanche Manager, see the reference guide for your mobile device.

---

- 2 Launch the Management Console and connect to the Agent.
- 3 In the Tree View of Management Console, locate and right-click the Telnet Client package.

A menu list appears.

- 4 Select `Configure Package`.



**Figure 2-2.** *Configuring the Telnet Client Package*

A menu list appears.

- 5 From the menu list, select the component of the Telnet Client that you want to configure:
  - Select `Host Profiles` to access the *Host Profiles* dialog box, which will allow you to configure host profiles and SSL settings for the Telnet Client.

---

**NOTE** For more information about configuring host profiles, see *Chapter 3: Host Profiles* on page 29.

---

- Select `Emulation Parameters` to access Configuration Manager, which will allow you to modify emulation parameters for the Telnet Client.

---

**NOTE** For more information about configuring emulation parameters, see *Chapter 4: Emulation Parameters* on page 61.

---

- Select `Script Editor` to access the script editor, which will allow you to import and configure scripts for the Telnet Client.

---

**NOTE** For more information about configuring scripts, see *Chapter 5: Scripting* on page 77.

---

- Select `Keyboard Creator` to access the Keyboard Creator, which will allow you to create and import virtual keyboards for the Telnet Client.

---

**NOTE** For more information about using the Keyboard Creator, see *Chapter 6: Keyboard Creator* on page 101.

---

- Select `Resource Editor` to access the Resource Editor, which will allow you to import and deploy graphic and sound files.

---

**NOTE** For more information about using the Resource Editor, see *Chapter 7: Resource Editor* on page 113

---

- Select `Localization` to configure the Localization settings for the Telnet Client.
- 6 After you have configured the new settings for the Telnet Client, use Avalanche Manager to deploy the new configuration to the mobile device.



---

**NOTE** For information about deploying Telnet Client configurations to the mobile device, see *Deploying Configurations* on page 24.

---

## Using Microsoft ActiveSync to Configure the Telnet Client

Use the Microsoft ActiveSync installation and configuration utility to configure host profiles, emulation parameters, and localization. After you have created the configuration, push the configuration files to the mobile device over a Microsoft ActiveSync connection between the host system and the mobile device.

### To configure the Telnet Client using Microsoft ActiveSync:

- 1 Ensure that the Microsoft ActiveSync Telnet Client installation and configuration utility is installed on the host system.

---

**NOTE** For more information about installing and using the Microsoft ActiveSync installation and configuration utility, see the Telnet Client reference guide for your mobile device.

---

- 2 Launch the installation and configuration utility on the host system.

The *Wavelink Product Configuration* dialog box appears.

- 3 Click the icon button for the Telnet Client component that you want to configure:
  - Click the `Host Profiles` icon button to access the *Host Profiles* dialog box, which will allow you configure host profiles and SSL settings for the Telnet Client.

---

**NOTE** For more information about host profiles, see *Chapter 3: Host Profiles* on page 29.

---

- Click the `Emulation Parameters` icon button to access *Configuration Manager*, which will allow you to configure emulation settings for the Telnet Client.

---

**NOTE** For more information about emulation parameters, see *Chapter 4: Emulation Parameters* on page 61.

---

- Click the `Localization` icon button to access the *Localization* dialog box, which will allow you to configure localization settings for the Telnet Client.
- 4** After you have created the new configuration for the Telnet Client, use the installation and configuration utility to download the new configuration files to the mobile device over an ActiveSync connection between the host system and the mobile device.

---

**NOTE** For more information about deploying configuration, see *Deploying Configurations* on page 24.

---

## Deploying Configurations

This section provides the following information:

- Deploying Telnet Client configurations via Avalanche Manager
- Deploying Telnet Client configurations via Microsoft ActiveSync

### Deploying Configurations via Avalanche Manager

Use the Avalanche framework to deploy new Telnet Client configurations to the mobile device.

Deploying Telnet Client configurations to the mobile device involves the following tasks:

- 1** Prepare Avalanche Manager and the Avalanche Enabler on the mobile device for the update.
- 2** Create a connection to download the configuration to the mobile device.

### Preparing for Updates

Avalanche Manager provides communication between the Avalanche Agent and the Avalanche Enabler on the mobile device over the following media:

- Serial port
- RAPI (Microsoft ActiveSync)
- IP

---

**NOTE** RAPI support is available in Avalanche Manager 3.5 (or greater version). On the device-side, RAPI connections are supported available for mobile devices with a 3.5 (or greater) version of the Avalanche Enabler and for some pre-3.5 Avalanche Enablers.

---

Before you can create a connection between the Avalanche Agent and the mobile device over which the new configuration will be download, you must prepare both the mobile device and Avalanche Manager for the update media.

Before you install the Telnet Client on a mobile device, ensure that the host system and the mobile device are properly configured.

Preparing the host system and the mobile device depends on the type of media that you are using to connect the host system to the mobile device.

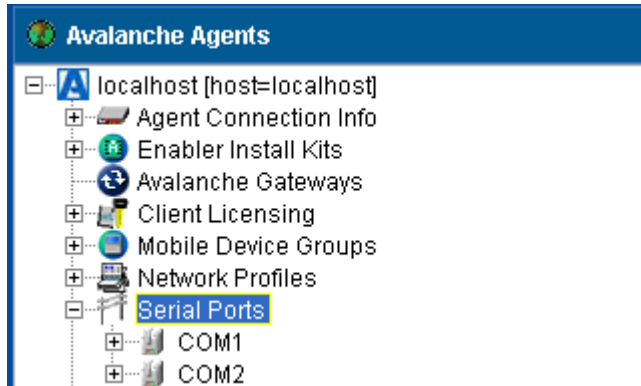
Avalanche Manager allows serial connections and RF connections.

### **Preparing for Serial Updates**

Use the following guidelines to prepare the serial connection between the mobile device and Avalanche Manager:

- Ensure that the Avalanche Enabler is installed and functioning properly on the mobile device.
- Ensure that the Avalanche Enabler on the mobile device is configured properly. If you have problems, verify the following:
  - The Avalanche Enabler is configured to use serial updates.
  - The Avalanche Enabler is configured with the IP address of the Avalanche Manager.
- Ensure that the software collection in which you have installed the Telnet Client software package is configured to allow RF updates.

- Ensure that Avalanche Manager is configured to use the serial port on the host system that is connected to the mobile device.

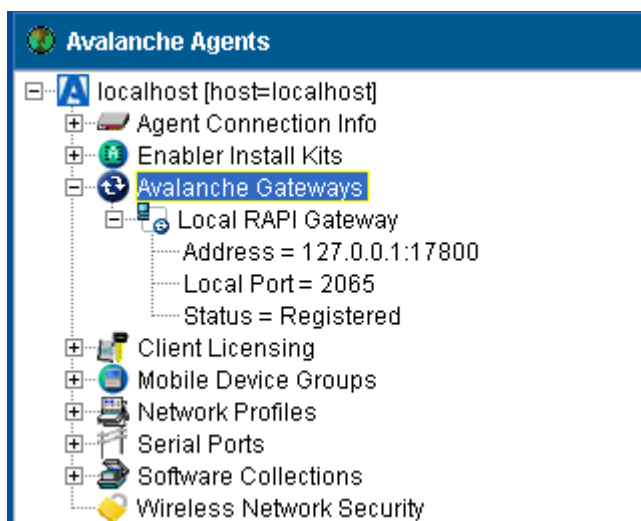


**Figure 2-3.** Serial Ports Enabled in Avalanche Manager

### Preparing for RAPI Updates

Use the following guidelines to prepare the RAPI connection between the mobile device and the Avalanche Manager:

- Ensure that your Avalanche Manager supports RAPI gateways. (RAPI gateways are available in Avalanche Manager 3.5 and greater versions.)
- Ensure that the Avalanche Enabler on the mobile device supports RAPI connections. (RAPI connections are supported in 3.5 and greater versions of the Avalanche Enabler.)
- Because RAPI gateways use Microsoft ActiveSync, ensure that you can create a Microsoft ActiveSync connection between the mobile device and the host system (that is, the system that hosts the Avalanche Agent).
- Ensure that you have created a RAPI gateway in Avalanche Manager.



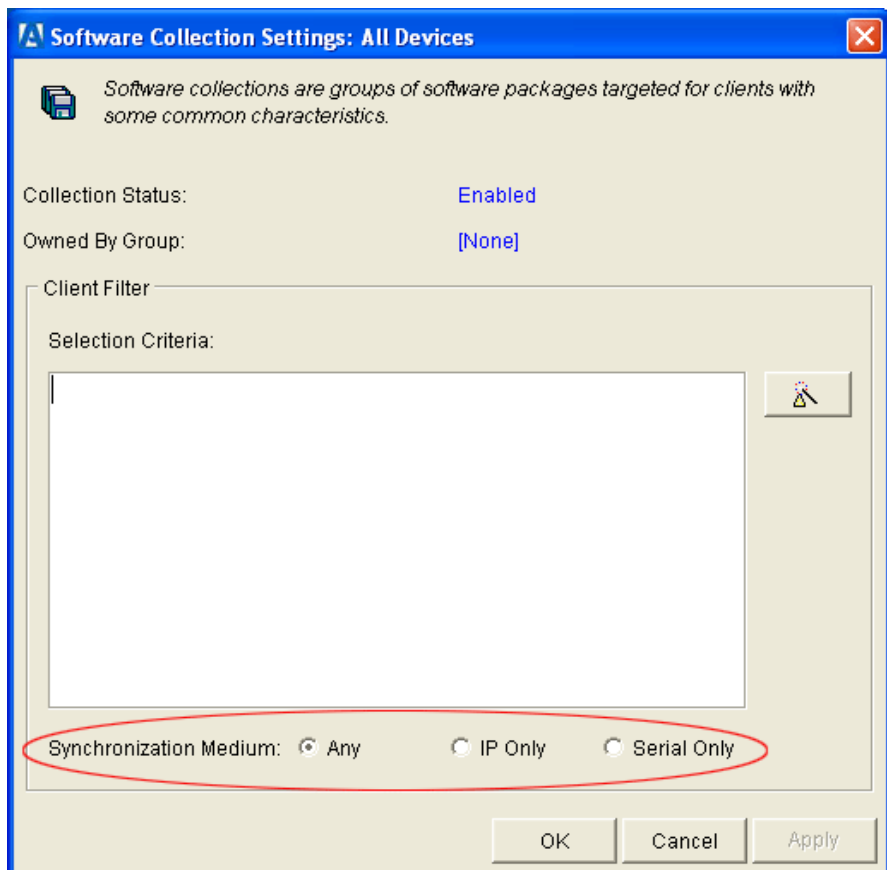
**Figure 2-4.** RAPI Gateway in Avalanche Manager

### Preparing for IP Updates

Use the following guidelines to prepare the IP connection between the mobile device and the Avalanche Manager:

- Ensure that the Avalanche Enabler is installed and functioning properly on the mobile device.
- Ensure IP connectivity between the mobile device and the host system. If you have problems, verify the following:
  - The host system has a valid IP address.
  - The mobile device has a valid IP address.
  - The mobile device is configured with the correct ESSID.
  - The mobile device is using the correct WEP key, if WEP is enabled on the wireless LAN.
  - The host system has a valid IP route to the mobile device.
  - The mobile device has a valid IP route to the host system.

- Any firewalls between the host system and the mobile device are configured to allow TCP traffic to port 1779 (the port that Avalanche uses for TCP communication).
- Ensure that the Avalanche Enabler on the mobile device is configured with the correct IP address of the Avalanche Manager.
- Ensure that the synchronization settings for the selection criteria for the software collection to which the Telnet Client package belongs allows IP synchronization (Figure 2-5).



**Figure 2-5.** Setting the Software Collection Synchronization Medium

### Downloading the Configuration to the Mobile Device

After you have prepared the synchronization medium, create a connection between the Avalanche Agent and the mobile device to download the new configuration.

#### To deploy the new configuration to the mobile device:

- 1 Launch Avalanche Manager and connect to the Agent.
- 2 In the Avalanche Agents tree, locate and right-click the Telnet Client software package.

A menu list appears.

- 3 From the menu list, select `Enable Package`.

The software package is enabled and ready to download to mobile devices.

- 4 Use one of the following methods to update the client:

- From the Avalanche Enabler on the mobile device, select `File > Connect`.
- In the Device View of Avalanche Manager, right-click the mobile device and select `Update Now (Allow User Override)` or `Update Now (Disallow User Override)`.

---

**NOTE** You cannot use `Update Now` to force an update over a serial or RAPI connection. Serial connections must be initiated from the mobile device. RAPI updates occur whenever a Microsoft ActiveSync connection is initiated between a mobile device and the host system.

---

- Wait for the mobile device to perform a periodic update according to the Avalanche Enabler configuration on the mobile device.
- Wait until Avalanche Manager instructs the mobile device to perform an update, which occurs according to the Scheduled Updates configuration of Avalanche Manager.

- For RAPI updates, connect the mobile device to the host system in a manner that will initiate a Microsoft ActiveSync connection between the mobile device and the host system.

When you create the connection between the host system and the mobile device, the configuration files are downloaded to the mobile device.

---

**NOTE** Only the configuration files that have changed are pushed down to the mobile device. The new configuration files replaced (overwrite) the existing configuration files on the device.

---

## Deploying Configurations via Microsoft ActiveSync

Use a Microsoft ActiveSync connection between the host system and the mobile device to download new Telnet Client configurations to the mobile device.

### To deploy a new configuration to the mobile device using Microsoft ActiveSync:

- 1 Ensure that you have a Microsoft ActiveSync between the host system and the mobile device.

---

**NOTE** For more information about using Microsoft ActiveSync, see *Appendix A: Using Microsoft ActiveSync* on page 221.

---

- 2 Launch the Microsoft ActiveSync Telnet Client installation and configuration utility.

The *Wavelink Product Configuration* dialog box appears.

- 3 Click `Config Only`.

The new configuration is downloaded to the mobile device. Any existing Telnet Client configuration files on the mobile device are overwritten.

---

**NOTE** All configuration files, including those for host profiles, emulation parameters, and localization settings are downloaded to the mobile device when you click the `Config Only` button.

---



## Chapter 3: Host Profiles

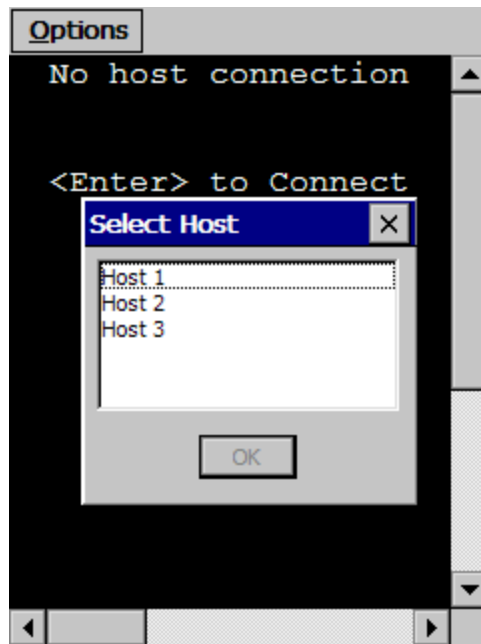
This section provides the following information:

- Overview of Host Profiles
- Configuring a Host Profile
- Host Profiles and SSL
- Host Profiles and Wavelink TermProxy
- Host Profile Settings

### Overview of Host Profiles

A host profile defines the parameters that the Telnet Client should use when it attempts to initiate a Telnet connection with a specific host. You may configure as many host profiles for the Telnet Client as you wish.

When a user at the mobile device attempts to use the Telnet Client to initiate a Telnet session with a host, the Telnet Client displays a list of available host profiles.



**Figure 3-1.** *Telnet Client Available Host Profiles*

The user selects the host to which they wish to connect, and the Telnet Client uses the host profile settings to attempt to establish a session with the host.

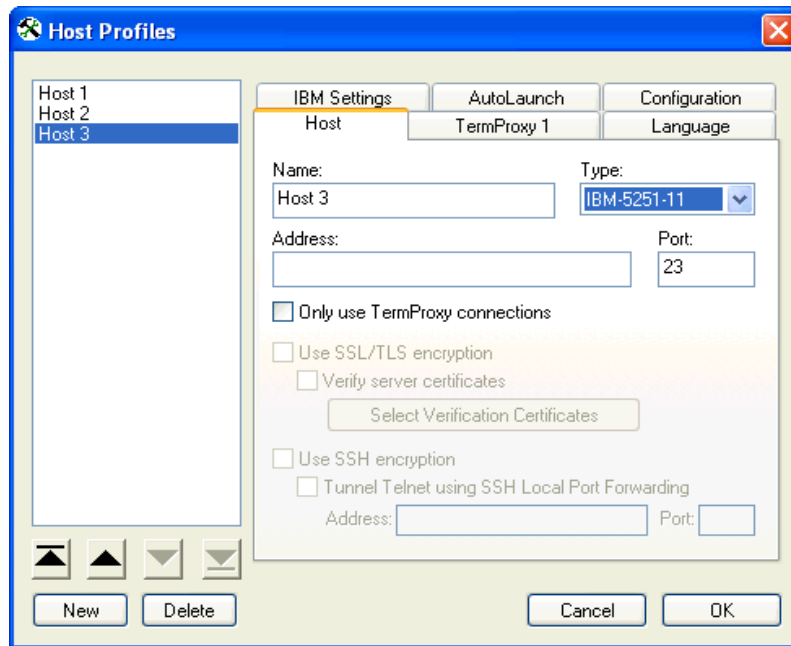
You may configure the following settings for a host profile:

- **Alias.** This is the alias of the connection. Use a name that adequately describes the host system to which the user is connecting.
- **Emulation Type.** This is the emulation type that the Telnet Client should use when connecting to the host system.
- **IP Address.** This is the IP address of the host system to which the user is connecting.
- **Port.** This is the TCP listening port of the host system.
- **SSL Settings.** You may select to protect the Telnet connection to the host system via SSL. You may also configure the SSL connection for certificate validation and import trusted certificates.

- **TermProxy Settings.** You may configure the Telnet Client to connect to a Wavelink TermProxy server. You may define up to three TermProxy connections for failover purposes. You may configure the TermProxy connection to use SSL with certificate validation.
- **Language.** If your Telnet Client supports the language feature, you may configure the Telnet Client to display a certain set of characters while connected to the host system.
- **Workstation ID.** If you have configured the host profile for IBM-type emulation, then you may configure a unique and/or dynamic workstation ID that the Telnet Client will use when connecting to the host system.
- **Telnet Negotiation String.** If you have configured the host profile for VT-type emulation, then you may configure a Telnet negotiation string that the Telnet Client will use when connecting to the host system.
- **Autologin.** If you have configured the host profile for VT-type emulation, then you may configure autologin settings that the Telnet client will use when connecting to a host system.
- **Host-Specific Emulation Parameters.** You may configure host-specific emulation parameters. These parameters will override global emulation parameter settings during Telnet connections to the host system that the host profile specifies.

## Configuring a Host Profile

Use the *Host Profiles* dialog box to configure host profiles. See *Chapter 2: Installation and Configuration* on page 15 for information about using your specific installation and configuration utility to access the *Host Profiles* dialog box.



**Figure 3-2.** *Host Profiles Dialog Box*

Each host profile that you configure appears in the left panel of the *Host Profiles* dialog box. Use the arrow buttons at the bottom of the left panel to reorder profiles in the list.

The following tasks outline the process of configuring host profiles for the Telnet Client:

- 1 Access the *Host Profiles* dialog box.
- 2 Add, modify, or remove host profiles and save the changes.
- 3 Download the configuration to mobile devices.

When you save the host profiles that you have configured, the changes you have made are saved to a configuration file.

### **Adding a Host Profile**

You can use the *Host Profiles* dialog box to create a new host profile.

**To create a new host profile:**

- 1 Access the *Host Profiles* dialog box.
- 2 In the *Host Profiles* dialog box, click **New**.

Various tabs appear in the *Host Profiles* dialog box that allow you to configure the parameters for a new host profile. The tabs that appear are dependent on the type of emulation that you select for the host profile. The *Host Profiles* dialog box automatically defaults to an IBM 5250 emulation type.

- 3 Use the tabs in the *Host Profiles* dialog box to configure the host profile.

The name (alias) of the host profile appears in the left text box of the *Host Profiles* dialog box.

---

**NOTE** For information about the various tabs in the *Host Profiles* dialog box, see *Host Profile Settings* on page 48.

---

- 4 After you have finished configuring the host profile, click **OK**.

The new host profiles configuration is saved to the host system.

- 5 Download the new host profiles configuration to the mobile device.

---

**NOTE** For information about using the Microsoft ActiveSync utility or the Avalanche Telnet Client to download configurations to mobile devices, see *Deploying Configurations* on page 22.

---

---

**NOTE** To exit the *Host Profiles* dialog box without saving the changes that you have made, click **Cancel**.

---

**Modifying an Existing Host Profile**

You can use the *Host Profiles* dialog box to modify an existing host profile.

**To modify an existing host profile:**

- 1 Access the *Host Profiles* dialog box.

- 2 From the list of host profiles in the text box in the left of the dialog box, select the host profile that you want to modify.
- 3 Use the various tabs in the *Host Profiles* dialog box to configure the host profile.

---

**NOTE** For information about the parameters in the various tabs of the *Host Profiles* dialog box, see *Host Profile Settings* on page 48.

---

- 4 After you have finished modifying the host profile, click `OK`.  
The new host profiles configuration is saved to the host system.
- 5 Download the new host profiles configuration to the mobile device.

---

**NOTE** For information about using the Microsoft ActiveSync utility or the Avalanche Telnet Client to download configurations to mobile devices, see *Deploying Configurations* on page 22.

---

---

**NOTE** To exit the *Host Profiles* dialog box without saving the changes that you have made, click `Cancel`.

---

## Deleting a Host Profile

You can use the *Host Profiles* dialog box to delete an existing host profile.

- 1 Access the *Host Profiles* dialog box.
- 2 In the text box on the left side of the *Host Profiles* dialog box, select the host profile that you want to remove.
- 3 Click `Delete`.

The host profile is removed from the *Host Profiles* dialog box.

- 4 After you have finished configuring the host profile, click `OK`.  
The new host profiles configuration is saved to the host system.

- 5 Download the new host profiles configuration to the mobile device.

---

**NOTE** For information about using the Microsoft ActiveSync utility or the Avalanche Telnet Client to download configurations to mobile devices, see *Deploying Configurations* on page 22.

---

---

**NOTE** To exit the *Host Profiles* dialog box without saving the changes that you have made, click `Cancel`.

---

### Subnet-Specific Addresses

When creating a host profile, you may enter a subnet-specific address rather than an IP address or a DNS name. A subnet-specific Telnet address will have the following format: `0.X.X.X/X`. The specified address is combined with the mobile device IP address to determine the host's address. The number after the slash determines the number of bits of the subnet-specific address that should be ignored. This is usually the same as the number of bits at the start of the subnet mask.

Examples:

For a mobile device with an IP address of 10.20.30.40:

- When connecting to a subnet-specific address of 0.1.2.3/8, the device will look for a host at 10.1.2.3.
- When connecting to a subnet-specific address of 0.0.2.3/16, the device will look for a host at 10.20.2.3.
- When connecting to a subnet-specific address of 0.0.0.3/24, the device will look for a host at 10.20.30.3.

Subnet-specific addressing is also available for WEB emulation. However, you should use a `|` character instead of a `/` character to denote the number of bits.

Examples:

For a mobile device with an IP address of 10.20.30.40:

- When connecting to a subnet-specific address of `http://0.1.2.3|8`, the device will look for a host at `http://10.1.2.3/`.
- When connecting to a subnet-specific address of `https://0.0.0.3|24:8080/start.asp`, the device will look for a host at `https://10.20.30.3:8080/start.asp`.

## Host Profiles and SSL

The Telnet Client supports encryption-protect Telnet sessions via SSL. The Telnet Client supports SSL Telnet connections to host servers, as well as to the Wavelink TermProxy server.

---

**NOTE** Wavelink TermProxy provides SSL support for connections between the mobile device and the TermProxy server. Wavelink TermProxy does not support SSL connections between the TermProxy server and host systems.

---

The Telnet Client also supports certificate validation for SSL connections.

To enable and use SSL for the Telnet Client requires the following:

- Install the SSL support package on the host system.
- Install the SSL support package on the mobile device.
- Enable SSL for the host profile.
- Enable certificate validation for the host profile and import server certificates (optional, if you want to use SSL with certificate verification).

### Installing the SSL Support Package on the Host System

Before you can begin configuring SSL and SSL certificates from the installation and configuration utility that you are using, you must install the SSL support package on the host system.

The SSL support package is a self-extracting executable that installs the required files that will allow you to configure SSL and SSL certificates.



---

**NOTE** To obtain the SSL support package, please contact Wavelink customer service. *Appendix D: Wavelink Contact Information* on page 267 contains Wavelink contact information.

---

## Installing the SSL Support Package on the Mobile Device

The Telnet Client will not be able to initiate SSL connections with hosts until you install the SSL support package on the mobile device.

Use one of the following methods to deploy the SSL support package to the mobile device:

- **Avalanche Manager.** The SSL support package is available as an Avalanche software package.
- **Microsoft ActiveSync.** The SSL support package is available as a bundled package that you can deploy over a Microsoft ActiveSync connection between a host system and the mobile device.
- **Third-Party Application.** The SSL support package is available for some third-party deployment applications.

---

**NOTE** To obtain the SSL support package for the mobile device, please contact Wavelink customer service. *Appendix D: Wavelink Contact Information* on page 267 contains Wavelink contact information.

---

## Enabling SSL

SSL is enabled via the *Host Profiles* dialog box. It is enabled on a per-host profile basis.

When you configure a host profile to use SSL, the TCP port for the host profile is automatically changed to 992, which is the well-known port number for SSL Telnet communication. If the host system uses a different port, then change the port to the correct setting.

### To configure a host profile to use SSL:

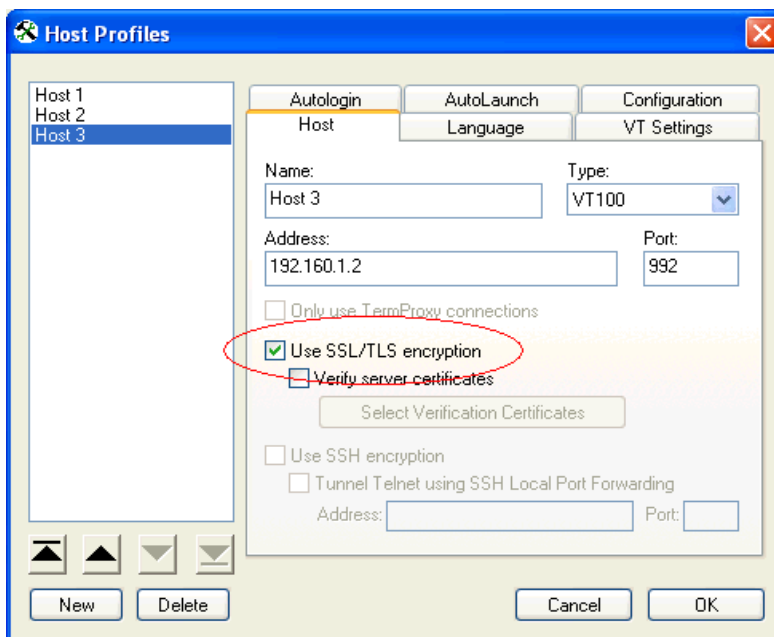
- 1 Access the *Host Profiles* dialog box.

- 2 From the left panel of the dialog box, select the host profile that you want to configure.
- 3 Depending on the connection requirements for the host profile, select one of the following:
  - If the host profile specifies a direct connection to a server, then enable the **Use SSL/TLS Encryption** option box in the Host tab.
  - If the host profile specifies a connection to a Wavelink TermProxy server, then enable the **Use SSL/TLS Encryption** option box in the TermProxy tab.

---

**NOTE** You will not be able to configure the **Use SSL/TLS Encryption** option box in the TermProxy tab until you select an option from the **TermProxy Server** menu list.

---



**Figure 3-3.** Enabling SSL for a Host Profile

- 4 After you have finished configuring the host profile, click **OK**.

The new host profiles configuration is saved to the host system.

- 5 Download the new host profiles configuration to the mobile device.

---

**NOTE** For information about using the Microsoft ActiveSync utility or the Avalanche Telnet Client to download configurations to mobile devices, see *Deploying Configurations* on page 22.

---

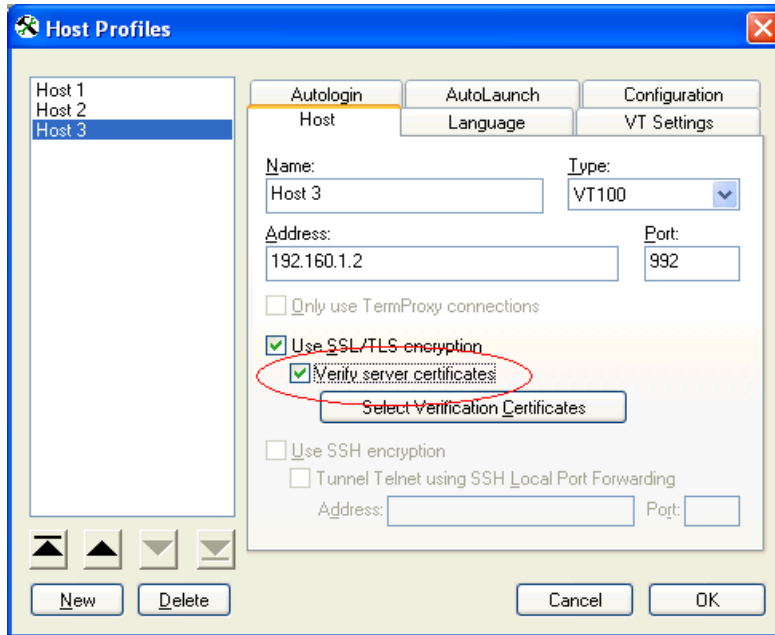
## Enabling Certificate Verification

When SSL is enabled, you may configure the Telnet Client to perform certificate verification. This prevents the Telnet Client from connecting to unauthorized servers.

Use the *Host Profiles* dialog box to import trusted certificates, which you can then download to the mobile device using the installation and configuration utility. When certificate verification is enabled for a host profile, the Telnet Client will test the credentials of the host system against the imported certificates and will refuse connections with host systems that present a certificate that is not in its list of imported certificates.

### To enable certificate validation and import valid certificates:

- 1 Access the *Host Profiles* dialog box.
- 2 From the left panel of the dialog box, select the host profile that you want to configure.
- 3 Depending on the connection requirements for the host profile, select one of the following:
  - If the host profile specifies a direct connection to a host, then enable the **Verify Server Certificates** option box in the Host tab.
  - If the host profile specifies a connection to a Wavelink TermProxy server, then enable the **Verify Server Certificates** option box in the TermProxy tab.

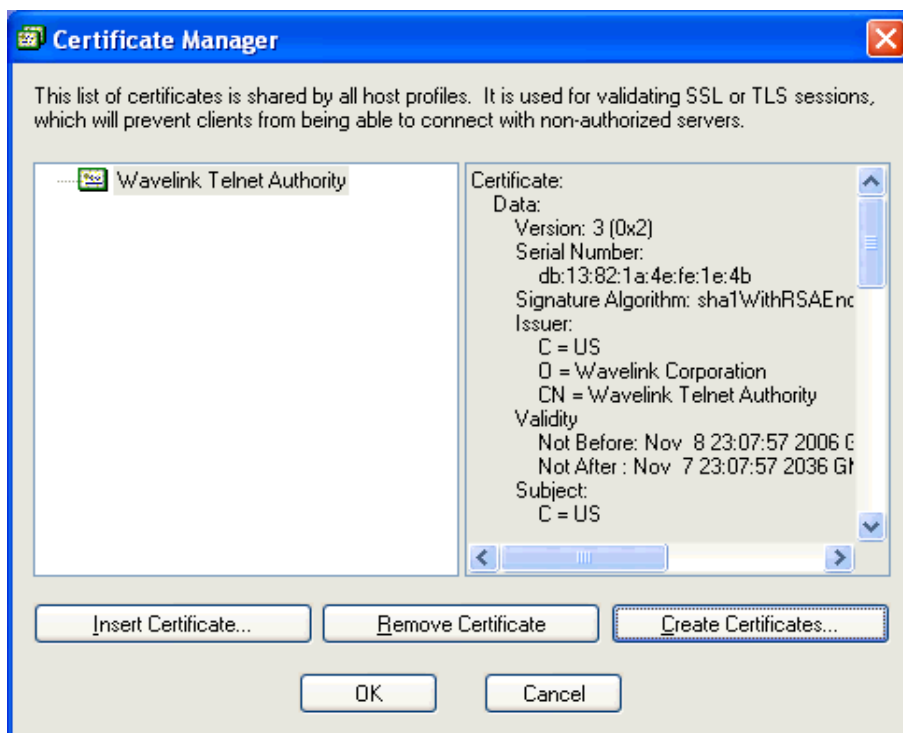


**Figure 3-4.** Enabling Certificate Validation

- 4 Click the corresponding `Select Verification Certificates` button.

The *Certificate Manager* dialog box appears.

- 5 Click `Insert Certificate...` to browse to and import a server certificate.
- 6 Click `Create Certificate...` to create a certificate and private key that you can then export to a TermProxy server or other host system.



**Figure 3-5.** Managing SSL Certificates

---

**NOTE** The certificates that you import and/or configure are available for all host profiles that you configure. The imported certificates should be considered a database or list of certificates against which the Telnet Client will check when initiating an SSL Telnet session with a host. If the host does not present a certificate that is in the list, then the Telnet Client will not establish a connection with the host.

---

**7** After you have finished importing/configuring certificates, click **OK**.

The *Certificate Manager* dialog box closes.

**8** Click **OK** to close the *Host Profiles* dialog box and save your new host profile settings.

**9** Download the new host profiles configuration to the mobile device.

---

**NOTE** For information about using the Microsoft ActiveSync utility or the Avalanche Telnet Client to download configurations to mobile devices, see *Deploying Configurations* on page 22.

---

## Host Profiles and Wavelink TermProxy

The Telnet Client provides integration with Wavelink TermProxy.

Wavelink TermProxy provides proxy services, mainly for session persistence, between the Telnet Client and host systems.

---

**NOTE** For more information about Wavelink TermProxy, refer to *Wavelink TermProxy Version 4.0 User Guide*.

---

You may use the *Host Profiles* dialog box to configure the following:

- TermProxy-only connections
- TermProxy-failover connections

---

**NOTE** TermProxy support (via the *Host Profiles* dialog box) is only available in version 5.0 (and greater) of the Telnet Client. While TermProxy 2.x allows connections from any type of Telnet Client, TermProxy 3.x requires connections from a 5.0 (or greater) Telnet Client.

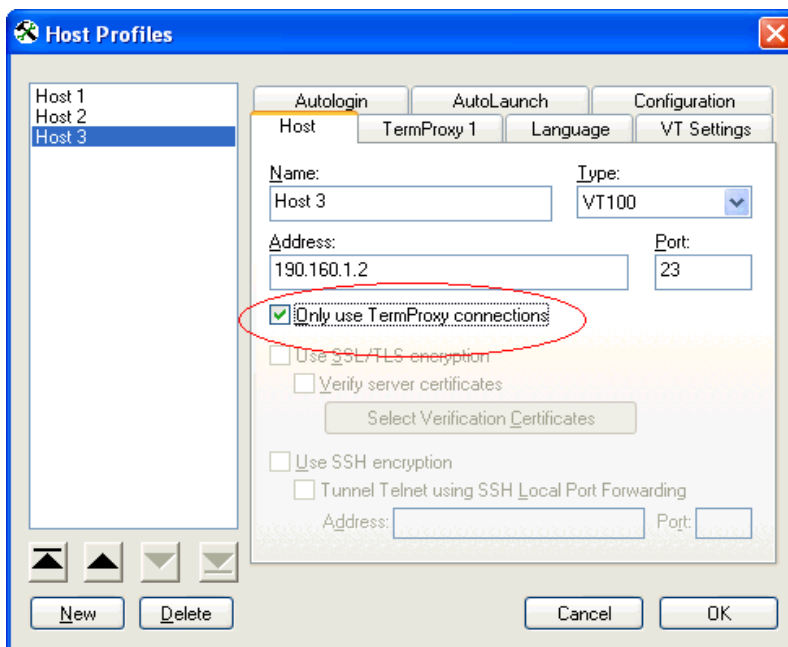
---

### Configuring a TermProxy-Only Connection

By default, if the Telnet Client cannot connect to the specified TermProxy server, then it will attempt a direct connection to the host. You may, however, configure the Telnet Client to only connect to a host through a Wavelink TermProxy server.

#### To configure a TermProxy-only connection to a host system:

- 1 Access the *Host Profiles* dialog box.
- 2 Select the host profile that you want to configure.
- 3 In the Host tab, enable the **Only Use TermProxy Connections** checkbox.



**Figure 3-6.** Enabling TermProxy-Only Connections

- 4 Use the TermProxy tab to configure the settings for the TermProxy server.

---

**NOTE** For more information about settings in the TermProxy tab, see *Host Profile Settings* on page 48.

---

- 5 After you have finished configuring the host profile, click **OK**.

The new host profiles configuration is saved to the host system.

- 6 Download the new host profiles configuration to the mobile device.

---

**NOTE** For information about using the Microsoft ActiveSync utility or the Avalanche Telnet Client to download configurations to mobile devices, see *Deploying Configurations* on page 22.

---

### **Configuring TermProxy Failover**

Use the TermProxy tabs in the *Host Profiles* dialog box to configure host and TermProxy failover. You may configure up to three failover connections for a host profile.

When the Telnet Client attempts to use the host profile to initiate a connection with a host, it will attempt connections in the following order:

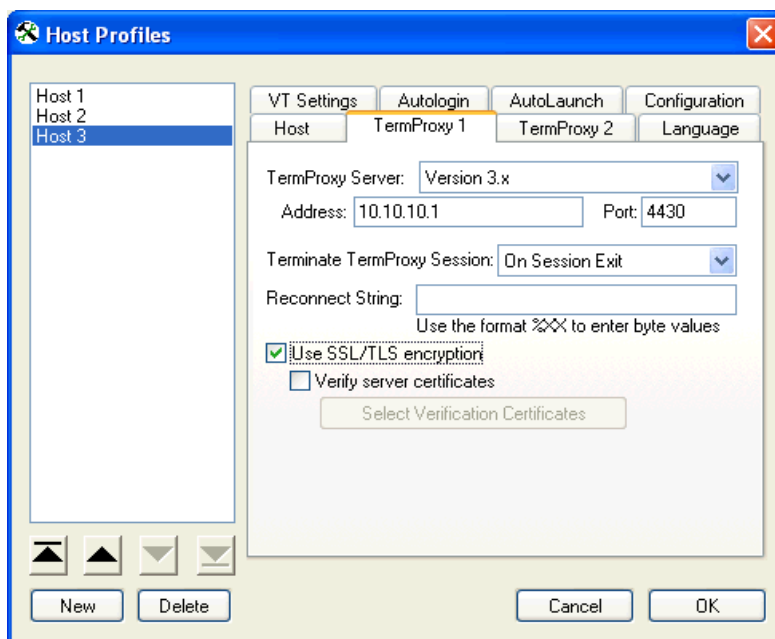
- Host specified in the Host tab of the host profile. (If you have specified a TermProxy-only connection, then it will attempt the host specified in the TermProxy 1 tab.)
- Host specified in the TermProxy 1 tab
- Host specified in the TermProxy 2 tab
- Host specified in the TermProxy 3 tab

If the Telnet Client is unable to contact any of the specified host, then it will return an error message.

#### **To configure TermProxy failure for a host profile:**

- 1** Access the *Host Profiles* dialog box.
- 2** Select the host profile for which you want to configure TermProxy failover.
- 3** Configure the Host tab.
- 4** Configure the TermProxy 1 tab.





**Figure 3-7.** Configuring the TermProxy Tab

- 5 Configure the TermProxy 2 tab
- 6 Configure the TermProxy 3 tab

---

**NOTE** For more information about the settings in the Host and TermProxy tabs, see *Host Profile Settings* on page 48.

---

- 7 After you have finished configuring the host profile, click **OK**.

The new host profiles configuration is saved to the host system.

- 8 Download the new host profiles configuration to the mobile device.

---

**NOTE** For information about using the Microsoft ActiveSync utility or the Avalanche Telnet Client to download configurations to mobile devices, see *Deploying Configurations* on page 22.

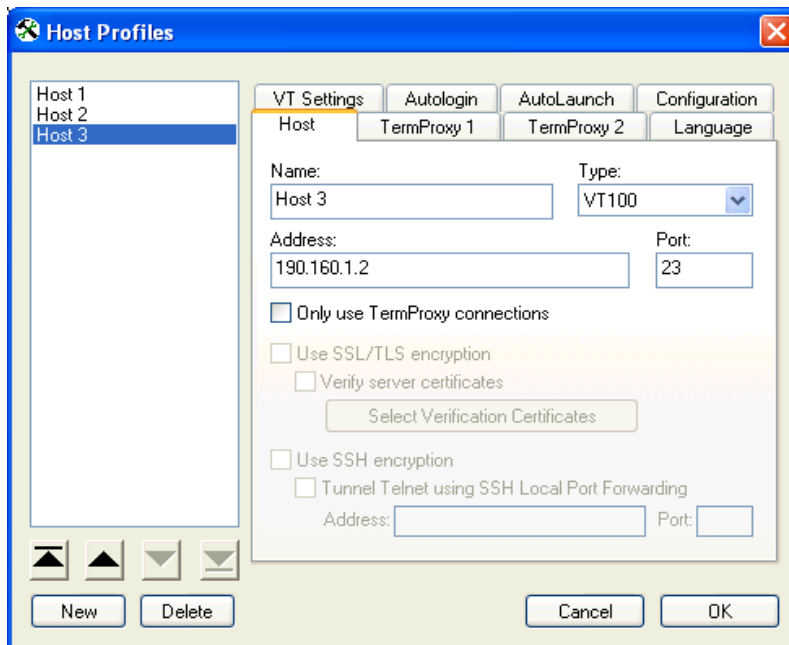
---

## Host Profile Settings

This section describes the parameters of each tab in the *Host Profiles* dialog box.

### Host Settings

Use the Host tab in the *Host Profiles* dialog box to configure the basic settings of the host profile.



**Figure 3-8.** Configuring Host Settings

The following list describes the options and configurable parameters in the Host tab.

<b>Name</b>	<p>Indicates the name of the host profile, which should be synonymous with the name (alias) of the host system to which the mobile device connects when the host profile is used.</p> <p><b>Possible Values:</b> 1 - 50 alpha-numeric characters</p> <p><b>Default Value:</b> New Host</p>
<b>Type</b>	<p>Indicates the type of emulation that the mobile device uses when connected to the host system.</p> <p><b>Possible Values:</b> &lt;IBM-5251-11&gt; &lt;IBM-3278-2&gt; &lt;IBM-3279-2&gt; &lt;IBM-3279-2-E&gt; &lt;VT100&gt; &lt;VT220&gt; &lt;HP&gt; &lt;WEB&gt;</p> <p><b>Default Value:</b> &lt;IBM-5251-11&gt;</p>
<b>Address</b>	<p>Indicates the IP address or host name of the host system to which the mobile device will connect.</p> <p><b>Possible Values:</b> Any valid IP address, host name, or web address.</p> <p><b>Default Value:</b> &lt;None&gt;</p>
<b>Port</b>	<p>Indicates the TCP port number on which the host system is listening for Telnet requests from clients.</p> <p><b>Possible Values:</b> 0 - 65535</p> <p><b>Default Value:</b> 23</p>

---

<b>Only Use TermProxy Connections</b>	<p>Indicates whether the Telnet Client should only connect to the host through a TermProxy server. If you enable this checkbox, you must configure the host information (name, IP address, emulation type, and port) and you must also configure the TermProxy 1 tab.</p> <p><b>Possible Values:</b> &lt;Enabled&gt; &lt;Disabled&gt;</p> <p><b>Default Value:</b> &lt;Disabled&gt;</p>
<b>Use SSL/TLS Encryption</b>	<p>Indicates whether the Telnet Client should use SSL to connect to the host system. When you enable SSL/TLS, the port will automatically change to 992, which is the well-known port for SSL Telnet communication.</p> <p><b>Possible Values:</b> &lt;Enabled&gt; &lt;Disabled&gt;</p> <p><b>Default Value:</b> &lt;Disabled&gt;</p>
<b>Verify Server Certificates</b>	<p>Indicates whether the Telnet Client should use certificate verification before allowing a connection to the host. If you enable certificate verification, then use Certificate Manager to import trusted server certificates and/or to create your own server certificates.</p> <p><b>Possible Values:</b> &lt;Enabled&gt; &lt;Disabled&gt;</p> <p><b>Default Value:</b> &lt;Disabled&gt;</p>
<b>Select Verification Certificates</b>	<p>Click this button to access the Certificate Manager, which allows you to import trusted server certificates and/or create your own server certificates for SSL certificate verification.</p>
<b>Use SSH encryption</b>	<p>Enable this option if you want to use SSH to encrypt the data between TermProxy and the host. If you enable this option, the <b>Use SSL/TLS encryption</b> option will disable.</p>
<b>Tunnel Telnet using SSH Local Port Forwarding</b>	<p>Enable this option if you want to connect to a standard Telnet by tunneling through a SSH server.</p>

<b>Address</b>	Enter the IP address of the SSH host that will perform the tunneling.
<b>Port</b>	Enter the port of the SSH host that will perform the tunneling.

## TermProxy Settings

You may configure up to three TermProxy connections. Use the TermProxy tabs to specify the parameters of the TermProxy connection.

The following list describes the configurable options in the TermProxy tab:

<b>TermProxy Server</b>	Select the TermProxy server to which the Telnet Client will connect.
-------------------------	--

**Possible Values:**

- **None.** Specifies no TermProxy or alternate host is used.
- **Version 2.x.** Specifies TermProxy 2.x. TermProxy 2.x will accept connections from any Telnet Client.
- **Version 3.x.** Specifies TermProxy 3.x. TermProxy 3.x will only accept connections from 5.x (or greater) Telnet Clients.
- **Version 4.x.** Specifies TermProxy 4.x.
- **Alternate Telnet Host.** Specifies an alternate host system for failover purposes.

**Default Value:** <None>

<b>Address</b>	Indicates the IP address of the TermProxy server or alternate host system.
----------------	--

**Possible Values:** Any valid IP address

**Default Value:** None

<b>Port</b>	<p>Indicates the TCP listening port of the TermProxy server or alternate host system.</p> <p><b>Possible Values:</b> 0 - 65535</p> <p><b>Default Value:</b> 4430</p>
<b>Terminate TermProxy Session</b>	<p>Indicates when the Telnet Client should terminate the connection to the TermProxy server.</p> <p><b>Possible Values:</b></p> <ul style="list-style-type: none"><li>• <b>Never.</b> The Telnet Client never terminates the session established with the TermProxy server. The TermProxy server is responsible for terminating the session.</li><li>• <b>On Network Error.</b> The Telnet Client terminates the session with the TermProxy server when a network error occurs, such as a loss of network connectivity.</li><li>• <b>On Session Exit.</b> The Telnet Client terminates the session with the TermProxy server when it disconnects from the host system.</li><li>• <b>Always.</b> The Telnet Client will terminate the session with the TermProxy server on a network error or when it disconnects from the host system.</li></ul> <p><b>Default Value:</b> &lt;On Session Exit&gt;</p>
<b>Reconnect String</b>	<p>Specifies the reconnect string that the mobile device should use when connecting to the host. (You may also configure reconnect strings in TermProxy.)</p> <p><b>Possible Values:</b> Any valid reconnect string</p> <p><b>Default Value:</b> None</p>

**Use SSL/TLS Encryption** Specifies whether the Telnet Client should use SSL to connect to the TermProxy server or alternate Telnet host. (TermProxy 2.x does not support SSL connections.)

**Possible Values:** <Enabled> <Disabled>

**Default Value:** <Disabled>

**Verify Server Certificates**

Indicates whether the Telnet Client should use certificate verification before allowing a connection to the TermProxy server or alternate Telnet host. If you enable certificate verification, then use Certificate Manager to import trusted server certificates and/or to create your own server certificates.

**Possible Values:** <Enabled> <Disabled>

**Default Value:** <Disabled>

**Select Verification Certificates**

Click this button to access the Certificate Manager, which allows you to import trusted server certificates and/or create your own server certificates for SSL certificate verification.

**Use Custom encryption** Enable the **Use Custom encryption** option to encrypt data between the mobile device and the TermProxy server.

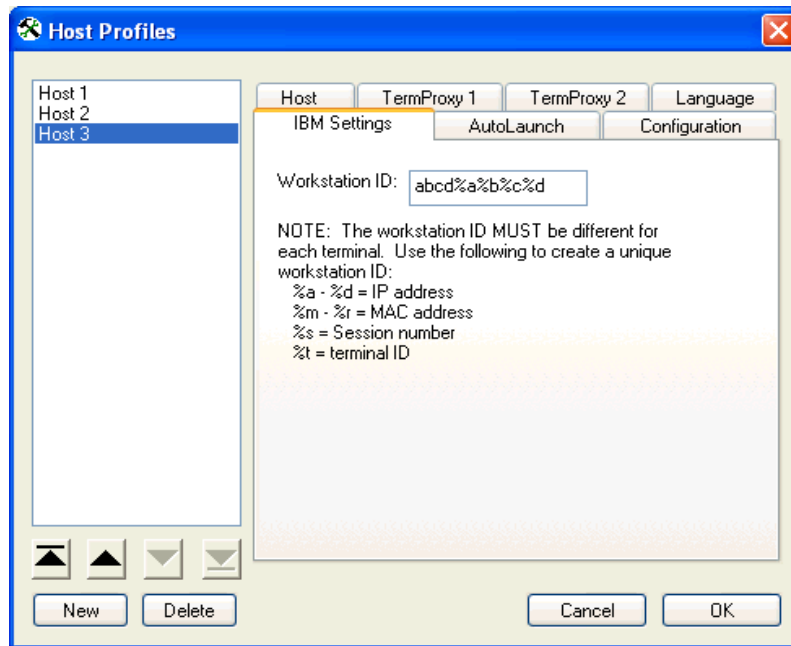
**Key**

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.

## **IBM Settings**

Use the IBM settings tab of the *Host Profiles* dialog box to configure the creation of a dynamic name for mobile devices that are loaded with this host profile.

The IBM Settings tab only appears you have configured the host profile for an IBM-type emulation in the Host tab.



**Figure 3-9.** *Configuring IBM Settings*



The following list provides information about the configurable parameters in the IBM Settings tab.

**Workstation ID**

Indicates the workstation ID that mobile devices use to connect to the host system. This includes static characters and the following switches, which are used to capture dynamic data that is specific to each mobile device:

- **%a - %d.** Captures specific octets of the IP address of the mobile device. For example, use %a%b%c%d to capture all four IP octets of the address of the mobile device, or use %d to capture only the last octet of the IP address of the mobile device.
- **%m - %r.** Captures specific octets of the MAC address of the mobile device. (For example, use %p%q%r to capture the last three octets of the MAC address of the mobile device.)
- **%s.** Captures the session number.
- **%t.** Captures the Avalanche terminal ID of the mobile device. (If the mobile device is not an Avalanche client, then this parameter is not valid.)

**Possible Values:** 0 - 20 alpha-numeric characters plus switches (see above)

**Default Value:** None

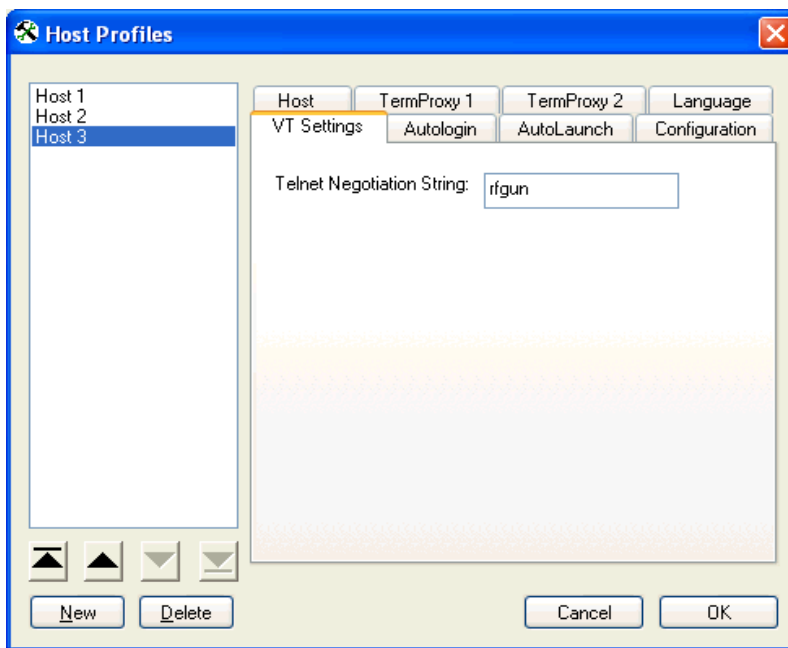
**NOTE:** IBM hosts usually truncate workstation IDs that are more than 10 characters. Also, the workstation ID should not begin with a numeric character.

**VT Settings**

Use the VT Settings tab in the *Host Profiles* dialog box to configure a Telnet negotiation string for the host connection.

A Telnet negotiation string allows you to specify the function or type of mobile device that is sending the Telnet request to the host system. The host system can then supply information to the mobile device based on Telnet negotiation string (for example, menus or display options).

The VT Settings tab only appears if you have configured the host profile for VT- or HP-type emulation in the Host tab.



**Figure 3-10.** *Configuring VT Settings*

The following list describes the configurable parameters in the VT Settings tab.

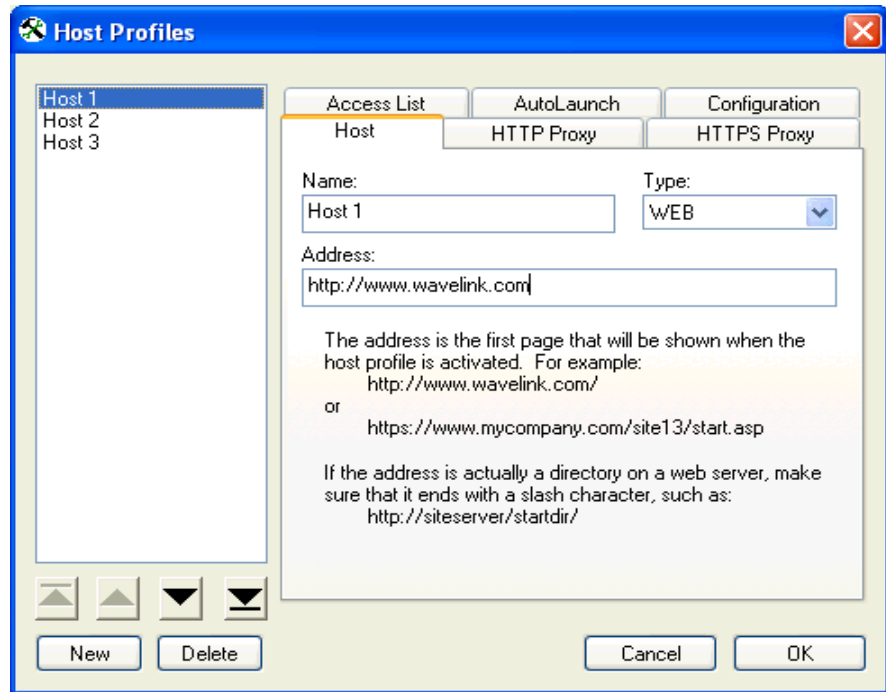
**Telnet Negotiation String** Specifies the Telnet negotiation string that the client should use when connecting to the host system.

**Possible Values:** 0 - 20 alpha-numeric characters

**Default Value:** <None>

## WEB Settings

When you configure the host profile for WEB-type emulation, various tabs appear offering different options for WEB settings.



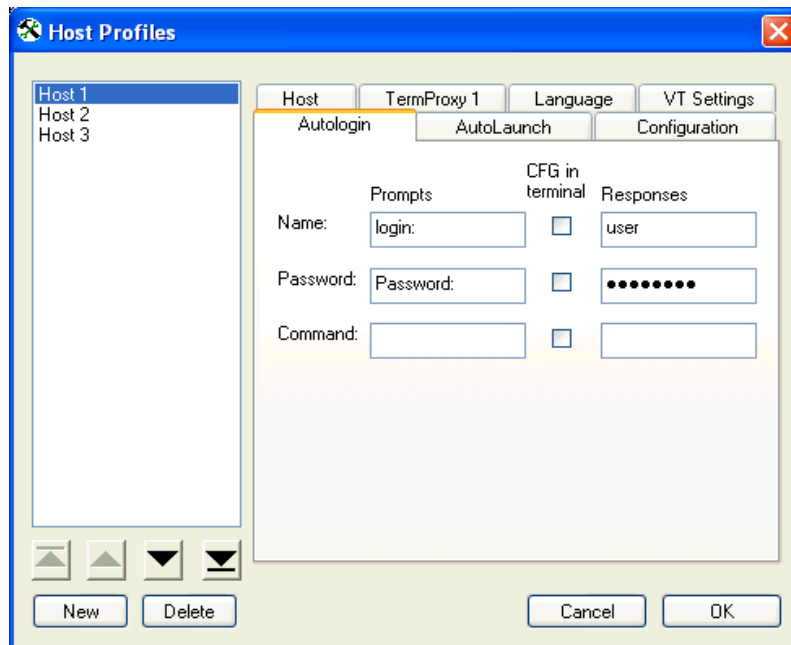
**Figure 3-11.** *Configuring WEB Settings*

For instructions on configuring each WEB settings tab, see *Industrial Browser Host Profile Settings* on page 158.

## Autologin Settings

Use the Autologin tab in the *Host Profiles* dialog box to configure autologin parameters for the mobile device, such as a user name and password.

The Autologin tab only appears if you have selected VT- or HP-type emulation for the host profile in the Host tab.



**Figure 3-12.** *Configuring Autologin Settings*

The following list describes the configurable options Autologin tab.

- Name - Prompts** Indicates the user name prompt that the host system uses.  
**Possible Values:** 0 - 60 alpha-numeric characters  
**Default Value:** login:
- Name - CFG in terminal** Indicates whether users should configure the response to the login prompt at the mobile device.  
**Possible Values:** <Enabled> <Disabled>  
**Default Value:** <Disabled>

---

<b>Name - Responses</b>	Indicates the response that the mobile device should send to the login prompt.  <b>Possible Values:</b> 0 - 30 alpha-numeric characters  <b>Default Value:</b> <None>
<b>Password - Prompts</b>	Indicates the password prompt that the host system uses.  <b>Possible Values:</b> 0 - 60 alpha-numeric characters  <b>Default Value:</b> <None>
<b>Password - CFG in terminal</b>	Indicates whether users should configure the response to the password prompt at the mobile device.  <b>Possible Values:</b> <Enabled> <Disabled>  <b>Default Value:</b> <Disabled>
<b>Password - Responses</b>	Indicates the password that the mobile device should send to the host system at the password prompt.  <b>Possible Values:</b> 0 - 30 alpha-numeric characters  <b>Default Value:</b> <None>
<b>Command - Prompts</b>	Indicates the command prompt that the host system sends to the Telnet Client after the login is complete.  <b>Possible Values:</b> 0 - 60 alpha-numeric characters  <b>Default Value:</b> <None>

**Command - CFG in terminal**

Indicates whether users should configure the response to the command line prompt at the mobile device.

**Possible Values:** <Enabled> <Disabled>

**Default Value:** <Disabled>

**Command - Responses**

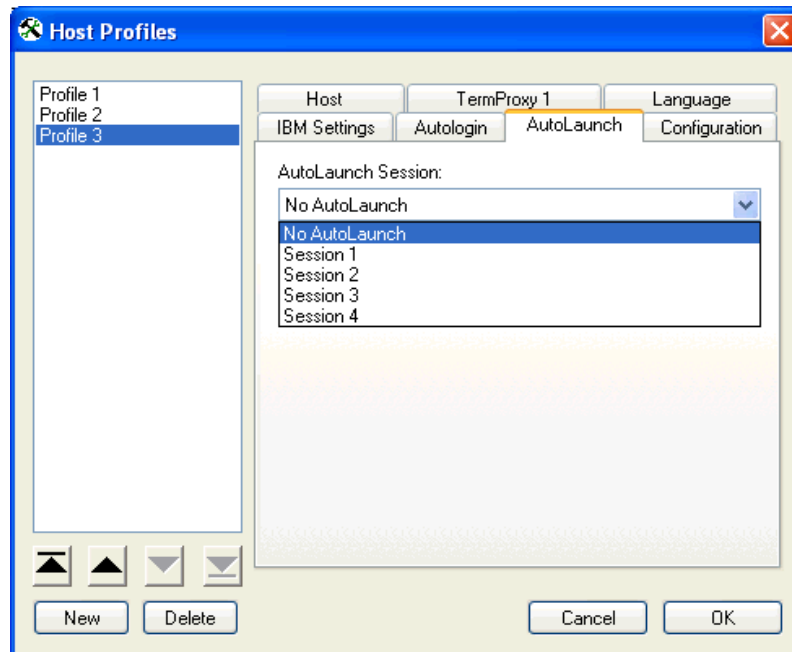
Indicates the command that the mobile device should send the host system at the command prompt.

**Possible Values:** 0 - 30 alpha-numeric characters

**Default Value:** <None>

**AutoLaunch Settings**

Use the AutoLaunch tab in the *Host Profiles* dialog box to configure the host profile to automatically launch when Telnet starts.



**Figure 3-13.** *Configuring AutoLaunch Settings*

The following options are available:

<b>No AutoLaunch</b>	Select this option to disable AutoLaunch.
<b>Session 1</b>	Select this option to automatically launch the Session 1 host profile.
<b>Session 2</b>	Select this option to automatically launch the Session 2 host profile.
<b>Session 3</b>	Select this option to automatically launch the Session 3 host profile.
<b>Session 4</b>	Select this option to automatically launch the Session 4 host profile.

Telnet will automatically launch the first profile in the host profiles list that is configured for AutoLaunch. If you want to automatically launch more than one profile, you must increase the number of sessions specified in the emulation parameters. For more information, see *Configuring the Number of Concurrent Sessions* on page 237.

To launch the next host profile in the list, select `Term` and then the desired session from the Telnet main menu.

---

**NOTE** Each host profile is automatically launched only once each time the program runs.

---

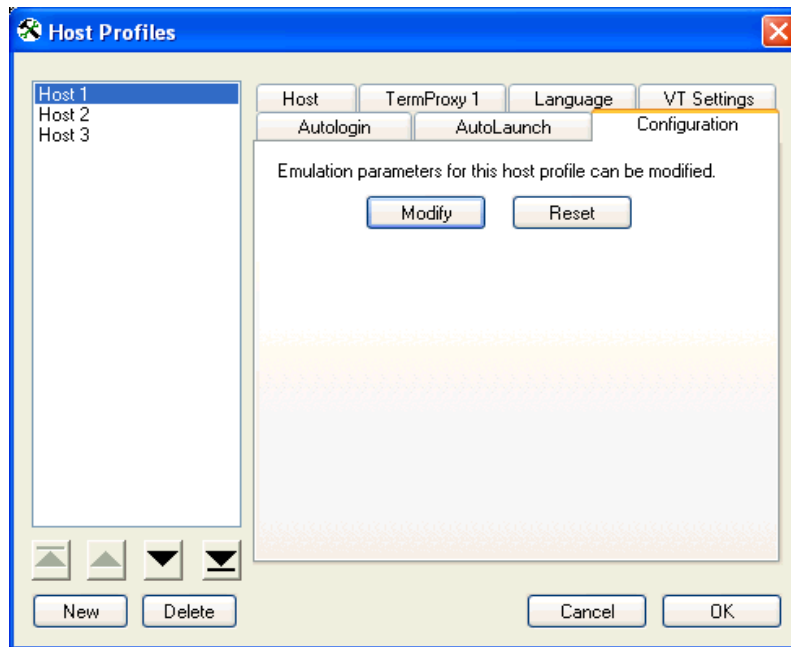
## Configuration Settings

Use the Configuration tab in the *Host Profiles* dialog box to access and configure per-host emulation parameters.

---

**NOTE** For more information about global and per-host emulation parameters, see *Chapter 4: Emulation Parameters* on page 61.

---



**Figure 3-14.** *Configuring Per-Host Emulation Settings*

The following list describes the options in the Configuration tab.

- Modify** Click this button to access Configuration Manager and modify the emulation parameters for the host connection.
- Reset** Click this button to reset the emulation parameters for the host connection back to the default settings.



## Chapter 4: Emulation Parameters

This section provides the following information:

- About Emulation Parameters
- Configuring Emulation Parameters
- Using Configuration Manager

### About Emulation Parameters

The Telnet Client allows you to configure emulation parameters for host connections.

You make changes to emulation parameters with the Configuration Manager utility, which provides an organized list of the emulation parameters that you can modify.

Emulation parameters are divided into two groups:

- Per-host
- Global

#### About Per-Host Emulation Parameters

Per-host emulation parameters apply only to a specific host connection, as dictated by the host profile the Telnet Client is using to connect to the host system. You can access the emulation parameters for a specific host profile through the *Host Profiles* dialog box.

When you choose to modify per-host emulation parameters, you access and use Configuration Manager to modify the `Hostcfg.bin` configuration file. Configuration Manager displays the name of the file that it is modifying in the title bar.

---

**NOTE** Per-host parameters are a subset of parameters. Not all Telnet Client emulation parameters are available for modification on a per-host basis.

---

## About Global Emulation Parameters

Global emulation parameters apply to all of the host profiles with which you have configured a client. Per-host emulation parameter configurations preempt global emulation parameter configurations.

When you choose to modify global emulation parameters, you access and use Configuration Manager to modify the Termcfg.bin configuration file. Configuration Manager displays the name of the file that it is modifying in the title bar

## Configuring Emulation Parameters

This section provides information about accessing Configuration Manager to modify global and per-host emulation parameters.

### Overview of Configuring Emulation Parameters

The following tasks outline the process of configuring emulation parameters:

- 1 Use the product configuration utility or the Telnet Client Avalanche software package to access the Configuration Manager.
- 2 Use the Configuration Manager to modify emulation parameters and save the new emulation parameters configuration file.
- 3 Download the new configuration file to the mobile device.

When you download the configuration file to the mobile device, any existing configuration file is overwritten.

### Accessing Global Emulation Parameters

This section provides the following information:

- Using the Microsoft ActiveSync installation utility to access the Configuration Manager for global and parameters
- Using the Avalanche software package to access the Configuration Manager for global emulation parameters

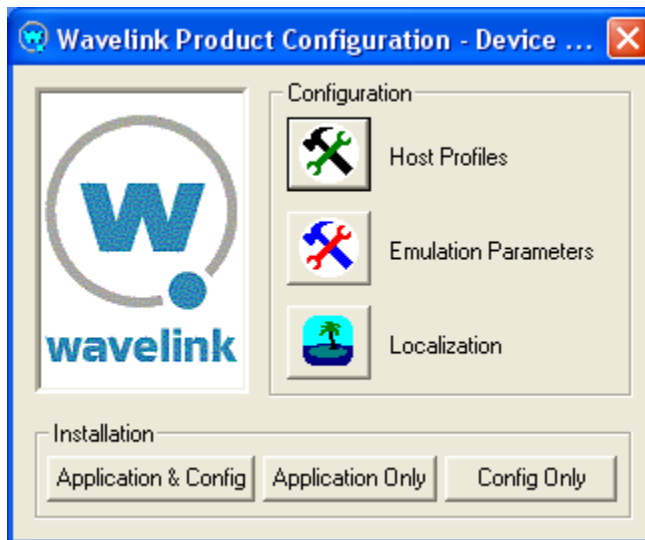
### Using Microsoft ActiveSync

If you used the product installation and configuration utility to install the Telnet Client to the mobile device via a Microsoft ActiveSync connection, use the same product installation and configuration utility to access the Configuration Manager and modify global emulation parameters.

#### To access global emulation parameters from the Microsoft ActiveSync utility:

- 1 On the host system, launch the Microsoft ActiveSync installation utility.

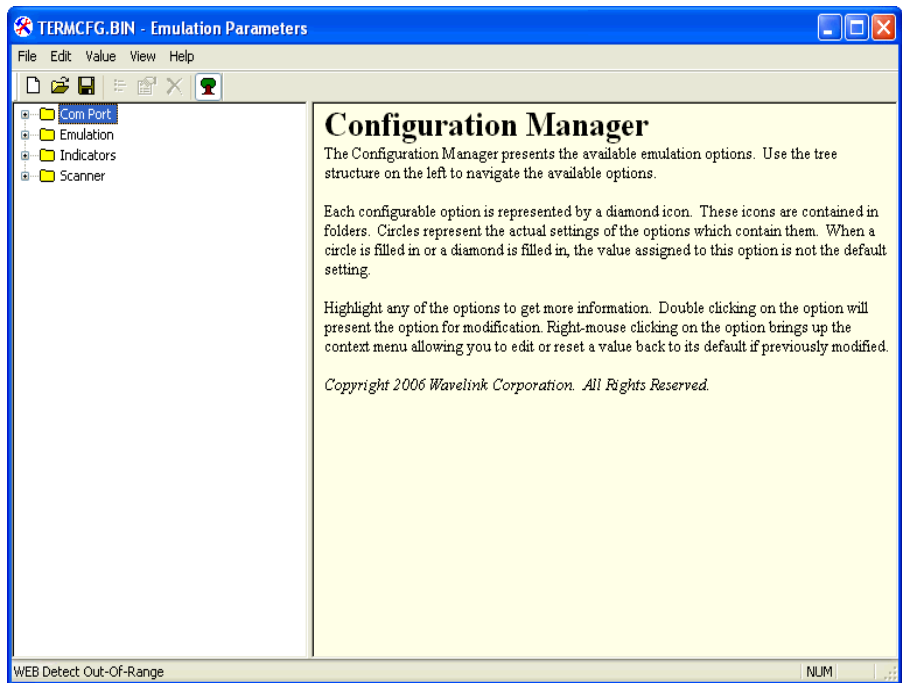
The *Wavelink Product Configuration* dialog box appears.



**Figure 4-1.** *Wavelink Product Configuration Dialog Box*

- 2 Click the `Emulation Parameters` icon button.

The Configuration Manager appears.



**Figure 4-2.** Configuration Manager

- 3 Use the Configuration Manager to configure the global emulation parameters for the Telnet Client.

---

**NOTE** For information about using Configuration Manager, see *Using Configuration Manager* on page 72.

---

- 4 After you have configured the emulation parameters, use one of the following methods to save the configuration to the host system:
  - Click the `save` icon button in the Configuration Manager tool bar.
  - Select `File > Save`.
- 5 Close the Configuration Manager.
- 6 Download the new emulation parameters to the mobile device.

---

**NOTE** For more information about downloading configuration to mobile devices, see *Deploying Configurations* on page 22.

---

### Using Avalanche Manager

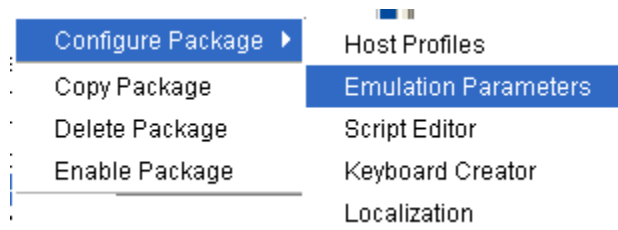
If you used Avalanche Manager to install the Telnet Client on the mobile device, use Avalanche Manager to access the Configuration Manager and modify global emulation parameters.

#### To access global emulation parameters from Avalanche Manager:

- 1 On the host system, launch Avalanche Manager and connect to the Agent.
- 2 In the Avalanche Agents tree, locate and right-click the Telnet Client software package.

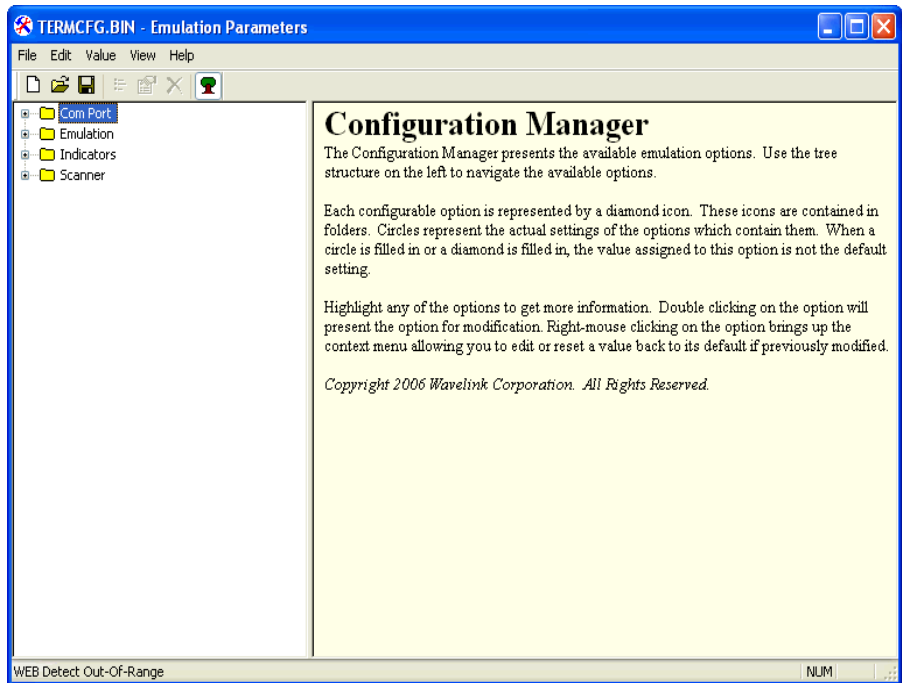
A menu list appears.

- 3 From the menu list, select `Configure Package > Emulation Parameters`.



**Figure 4-3.** *Configuring Emulation Parameters from Avalanche*

The Configuration Manager appears (4-4).



**Figure 4-4.** Configuration Manager

- 4 Use the Configuration Manager to configure the global emulation parameters for the Telnet Client.

---

**NOTE** For information about using the Configuration Manager, see *Using Configuration Manager* on page 72.

---

- 5 After you have configured the emulation parameters, use one of the following methods to save the configuration to the host system:
  - Click the `Save` icon button in the Configuration Manager tool bar.
  - Select `File > Save`.
- 6 Close the Configuration Manager.
- 7 Download the new emulation parameters to the mobile device.

---

**NOTE** For more information about downloading configuration to mobile devices, see *Deploying Configurations* on page 22.

---

## Accessing Per-Host Emulation Parameters

This section provides the following information:

- Using the Microsoft ActiveSync installation utility to access the Configuration Manager for per-host settings
- Using the Avalanche Telnet Client software package to access the Configuration Manager for per-host settings

Per-host emulation parameters are specific to a host connection and are accessed through the corresponding host profile in the *Host Profiles* dialog box.

### Using Microsoft ActiveSync

If you used the product configuration utility to install the Telnet Client on the mobile device via a Microsoft ActiveSync connection, use the same product configuration utility to access and configure per-host emulation parameters.

#### To access per-host emulation parameters from the Microsoft ActiveSync utility:

- 1 On the host system, launch the Microsoft ActiveSync installation utility.

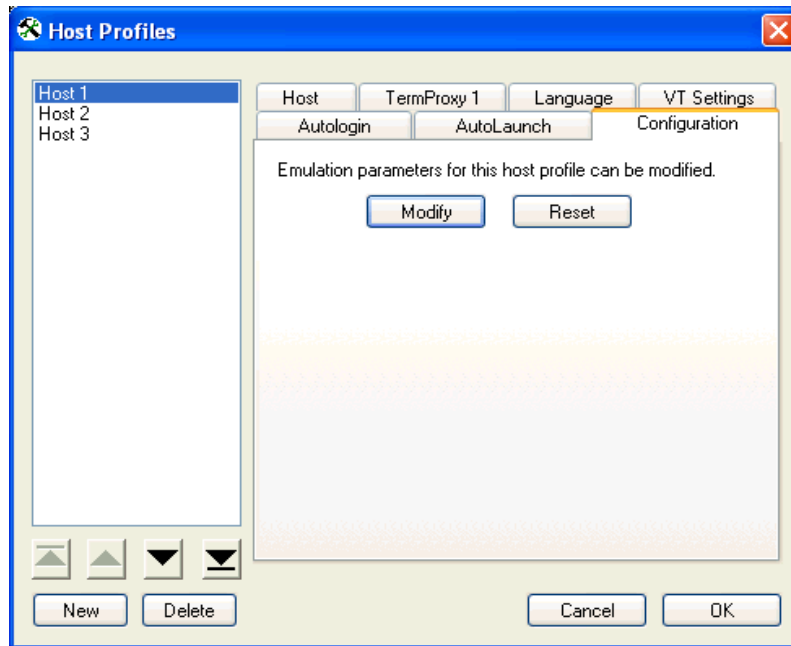
The *Wavelink Product Configuration* dialog box appears.

- 2 Click the `Host Profiles` icon button.

The *Host Profiles* dialog box appears.

- 3 From the list of host profiles, select the host profile that you want to configure.

- 4 Select the `Configuration` tab.



**Figure 4-5.** Selecting to Configure Per-Host Emulation Parameters

- 5 Click `Modify`.

The Configuration Manager appears.

- 6 Use the Configuration Manager to configure emulation parameters for the host profile that you have selected.

---

**NOTE** For information about using Configuration Manager, see *Using Configuration Manager* on page 72.

---

- 7 After you have configured the emulation parameters, use one of the following methods to save the configuration to the host system:
  - Click the `Save` icon button in the Configuration Manager tool bar.
  - Select `File > Save`.
- 8 Close the Configuration Manager.



- 9 Close the *Host Profiles* dialog box.
- 10 Download the new emulation parameters to the mobile device.

---

**NOTE** For more information about downloading configuration to mobile devices, see *Deploying Configurations* on page 22.

---

### Using Avalanche Manager

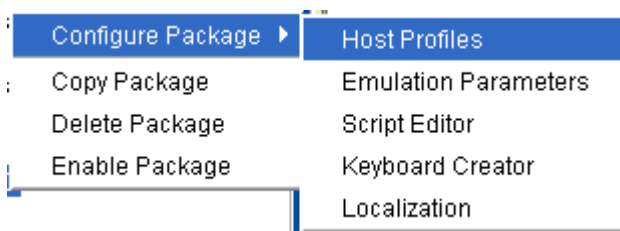
If you used Avalanche Manager to deploy the Telnet Client to the mobile device, use the Telnet Client software package in Avalanche Manager to access and configure per-host emulation parameters.

#### To access per-host emulation parameters from Avalanche Manager:

- 1 On the host system, launch Avalanche Manager and connect to the Agent.
- 2 In the Avalanche Agents tree, locate and right-click the Telnet Client software package.

A menu list appears.

- 3 From the menu list, select `Configure Package > Host Profiles`.



**Figure 4-6.** *Configuring Per-Host Emulation Parameters from Avalanche*

The *Host Profiles* dialog box appears.

- 4 From the list of host profiles, select the host profile that you want to configure.
- 5 Select the Configuration tab.
- 6 Click `Modify`.

The Configuration Manager appears.

- 7 Use the Configuration Manager to configure emulation parameters for the host profile that you have selected.

---

**NOTE** For information about using Configuration Manager, see *Using Configuration Manager* on page 72.

---

- 8 After you have configured the emulation parameters, use one of the following methods to save the configuration to the host system:
  - Click the `Save` icon button in the Configuration Manager tool bar.
  - Select `File > Save`.
- 9 Close the Configuration Manager.
- 10 Close the *Host Profiles* dialog box.
- 11 Download the new emulation parameters to the mobile device.

---

**NOTE** For more information about downloading configuration to mobile devices, see *Deploying Configurations* on page 22.

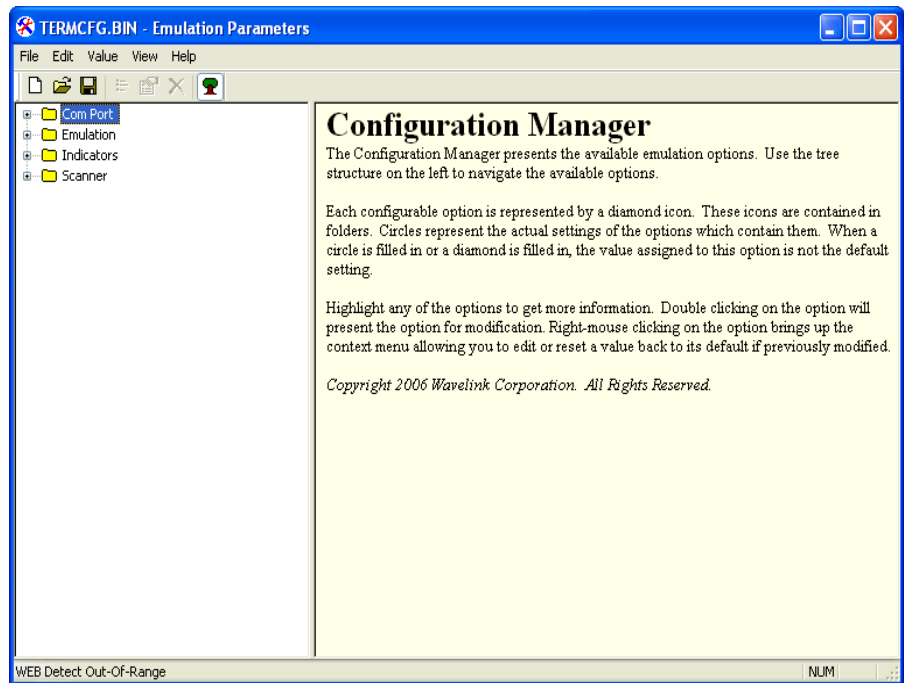
---

## Using Configuration Manager

This section provides the following information:

- An overview of Configuration Manager
- Using the Configuration Manager to modify emulation parameters
- Using the Configuration Manager find function

The Configuration Manager is the utility that allows you to modify global and per-host emulation parameters.



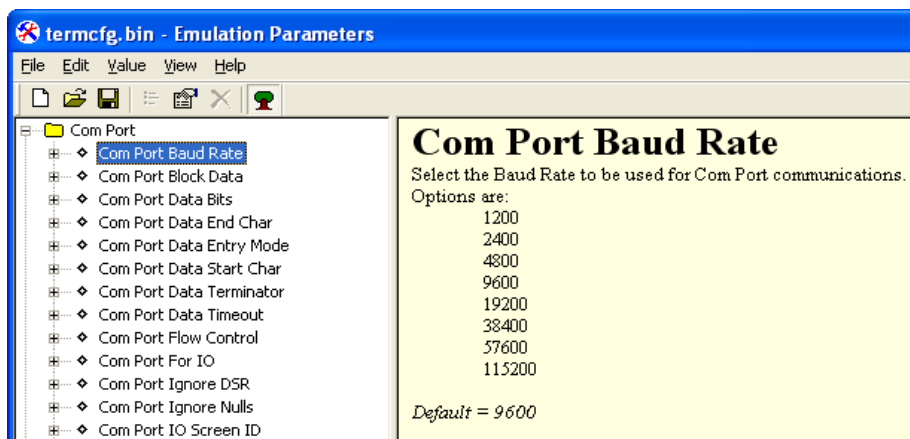
**Figure 4-7.** Configuration Manager

The left pane of the Configuration Manager displays the emulation parameters that you can modify. The emulation parameters are grouped by category.

The following list describes the different categories:

- |                  |  |
|------------------|--|
| <b>COM</b>       | Parameters in this category configure the function of the COM port on mobile devices.      |
| <b>Emulation</b> | Parameters in this category configure terminal emulation functions on mobile devices.      |
| <b>Scanner</b>   | Parameters in this category configure the function of bar code scanners on mobile devices. |

When you select a parameter in the left pane, information about the parameter displays in the right pane.



**Figure 4-8.** Emulation Parameter Information

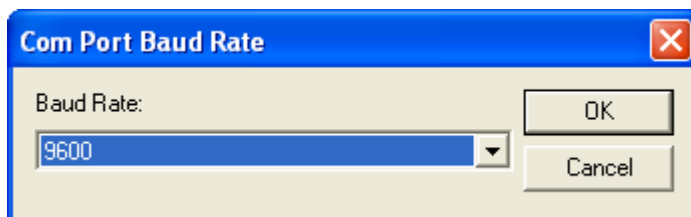
## Modifying Emulation Parameters

Determine the emulation parameters that you want to modify and use the Configuration Manager to make modifications.

### To modify an emulation parameter:

- 1 Access the Configuration Manager.
- 2 In the left pane of the Configuration Manager, locate the parameter that you want to modify.
- 3 Double-click the emulation parameter or right-click the emulation parameter and choose `Edit` from the menu list.

A dialog box appears that allows you to modify the parameter configuration.



**Figure 4-9.** Modifying an Emulation Parameter

- 4 Use the dialog box to configure the parameter.
- 5 After you have configured the parameter, click `OK` to keep the setting.

---

**NOTE** Click `Cancel` or the `Close` button to cancel any changes you have made.

---

- 6 Use one of the following methods to save the new configuration:
  - Click the `Save` icon button.
  - Select `File > Save`.
- 7 Close the Configuration Manager.
- 8 Download the new configuration to the mobile device.

---

**NOTE** For more information about deploying new Telnet Client configurations to mobile devices, see *Deploying Configurations* on page 22.

---

## Using the Find Function

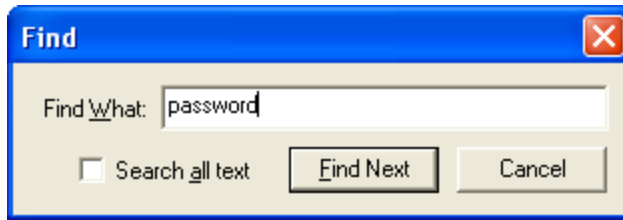
Use the Find function of the Configuration Manager to locate parameters or information by supplying a partial or full string that the Configuration Manager can use to locate the parameter or information that you want to find.

### To use the find function:

- 1 From the Configuration Manager **Edit** menu, select `Find`.

The *Find* dialog box appears.

- 2 Input a partial or full string for the parameter or information that you want to find.



**Figure 4-10.** *Inputting a String to Find*

- 3 Enable the **Search all text** checkbox to search not only the parameters, but also the help files.
- 4 Click `Find Next` to begin the search.

Continue to click `Find Next` until you locate the parameter or information for which you are searching.

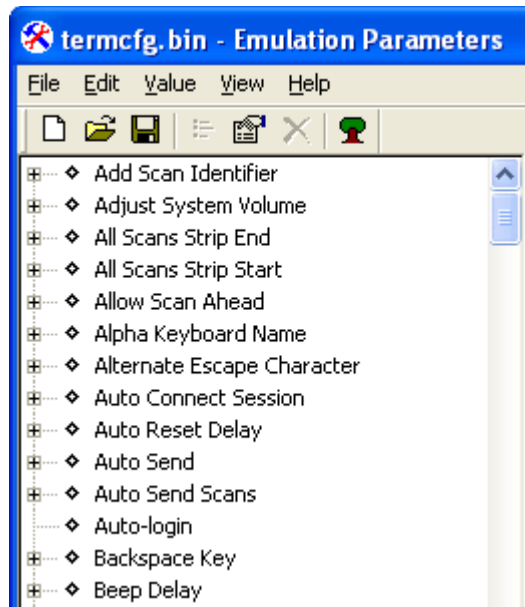
### **Switching to Alphabetized View**

By default, emulation parameters are displayed in a hierarchical tree view. You may switch to an alphabetized view, if you desire. When the alphabetized view is enabled, the Configuration Manager displays the emulation parameters in alphabetical order.

#### **To switch to the alphabetized view in Configuration Manager:**

- 1 In the Configuration Manager, access the **View** menu.
- 2 In the **View** menu, disable the `Tree Mode` option.

The Configuration Manager now displays the emulation parameters in an alphabetized list.



**Figure 4-11.** *Alphabetized View in the Configuration Manager*





## Chapter 5: Scripting

This section provides the following information

- Overview of Scripting
- Launching the Script Editor
- Creating Scripts Using the Script Editor
- Performing Script Capturing
- Field Data ID Button
- Editing Scripts
- Importing Scripts
- Saving and Exporting Scripts
- Deploying Scripts
- Executing Scripts

### Overview of Scripting

Wavelink Telnet Client includes a Script Editor that gives you the ability to create and execute scripts that automate processes on the Telnet Client.

---

**NOTE** The Script Editor is included in Telnet Client 5.1 and later versions.

---

The following steps outline the process of creating scripts using the Script Editor:

- 1 Launch the Script Editor.** You can launch the script editor Avalanche Manager.
- 2 Create a script using the Script Editor.** You can use the Script Editor to manually create the script code.

-Or-

**Create a script using the Script Capture option.** You can turn on Screen Capture and perform the actions you want included in your script.

- 3 Configure an execution method for your script.** You need to select from the available options the way you want to execute your script.
- 4 Execute your script from the Telnet Client.** Using the activation method you selected for the script, you can activate and execute your script.

Telnet Client allows one active script per emulation session. While one script is running, other scripts are not allowed to run. Scripts should be designed to do their action and then immediately exit. This allows the next script to run.

Scripts can only be run while a session is connected to a host. When a connection is dropped, the script is terminated. If you switch between sessions, the script running in the first session will be suspended until that session is returned to being active.

---

**NOTE** For detailed information about the using the Script Editor in Telnet Client, refer to the *Telnet Client Scripting Reference Guide*.

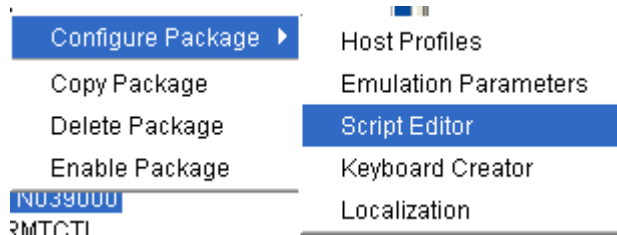
---

## Launching the Script Editor

If you are using Avalanche Manager to deploy the Telnet Client, you can launch the Script Editor from the Avalanche Manager. Then scripts created by or imported into the Avalanche Script Editor will automatically be deployed to the remote devices.

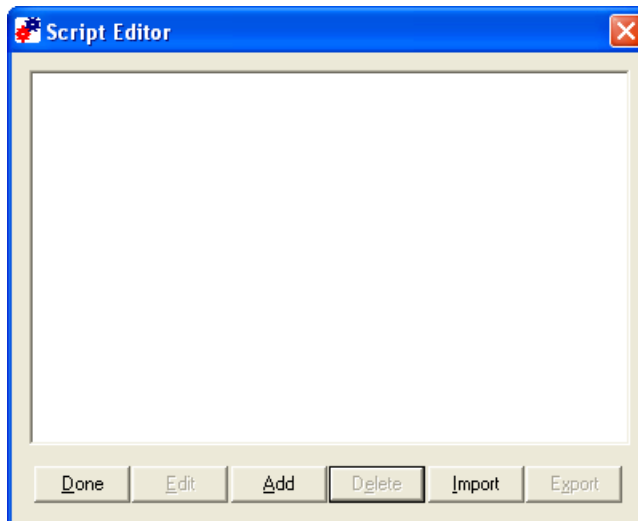
### To launch the Script Editor from Avalanche Manager:

- 1 Ensure the Telnet Client package is installed in Avalanche Manager.
- 2 From the Tree View in the Avalanche console, right-click the Telnet Client software package.
- 3 Select `Configure Package > Script Editor`.



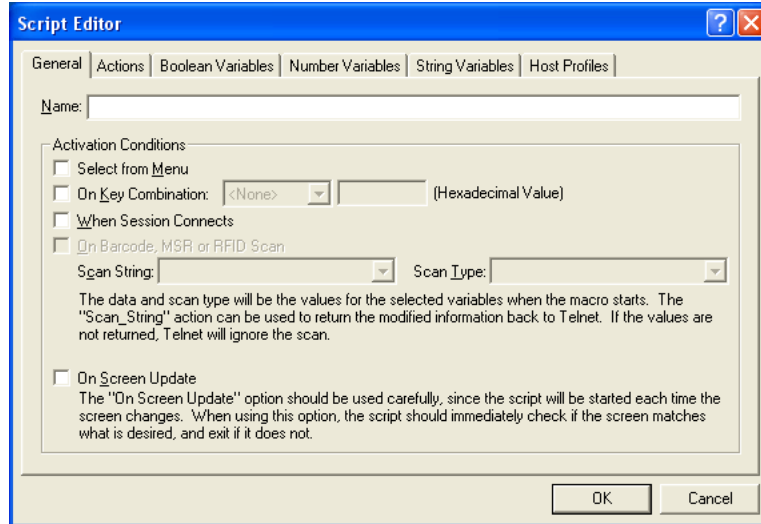
**Figure 5-1.** Launching the Script Editor from Avalanche Manager

The Script Editor opens.



**Figure 5-2.** Script Editor

- 4 Click **Add** to open the *Script Editor* configuration dialog box.



**Figure 5-3.** *Script Editor Configuration Dialog Box*

## Creating Scripts Using the Script Editor

This section provides information on how to create scripts manually using the Script Editor and includes the following information:

- Configuring the Script Name
- Selecting the Activation Method
- Creating the Script Code
- Creating Variables
- Selecting Host Profiles

Use the following steps to create a script manually:

- 1 Enter a script name and select an activation method.
- 2 Use the Actions tab to select actions and build the script code.
- 3 Use the Boolean Variables, Number Variables, or String Variables tabs to create Variables as needed to complete the script (not required).

- 4 Use the Host Profile tab to select host profiles that will be associated with this script.

## Configuring the Script Name

The script name is the name you will select from when activating the scripts.

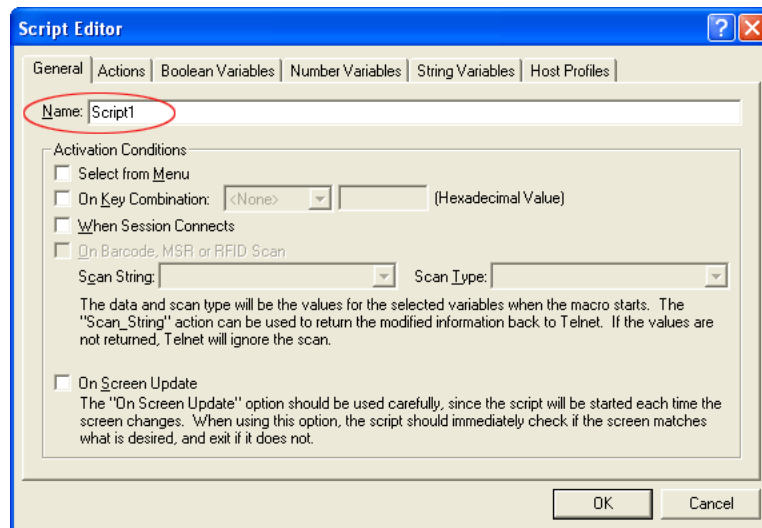


Figure 5-4. Entering the Script Name

## Selecting the Activation Method

You need to select how you want to activate your script, once it is created. A script with no activation method selected can still be called by another script, but it cannot be activated by itself.

This section provides information about assigning a method of activation to a script. The following is a list of the activation methods:

- Select from Menu
- On Key Combination
- When Session Connects
- On Barcode, MSR, or RFID Scan

- On Screen Update

### Select from Menu

Scripts with the **Select from Menu** option selected can be run using the menu option in the Telnet Client.

#### To configure the Select from Menu method:

- 1 Select the General tab or the Activate tab in the Script Editor.
- 2 Enable the **Select from Menu** option.

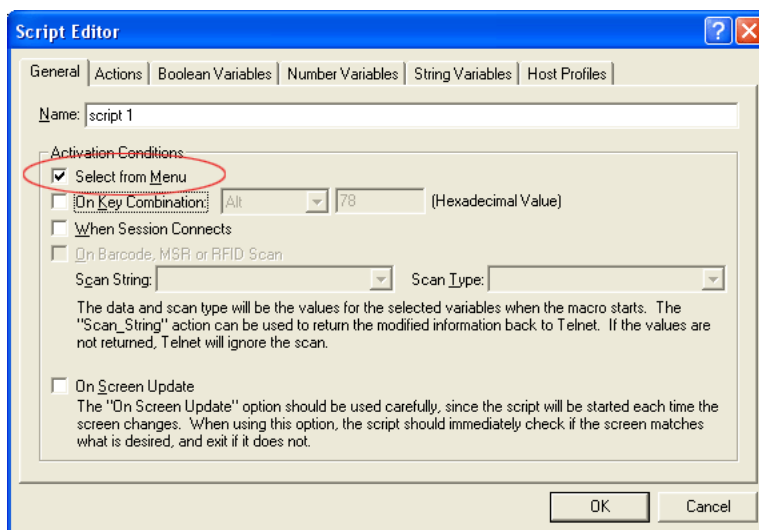


Figure 5-5. Select from Menu

- 3 Click **OK**.

### On Key Combination

This option lets you launch a script whenever a specific key combination is pressed.

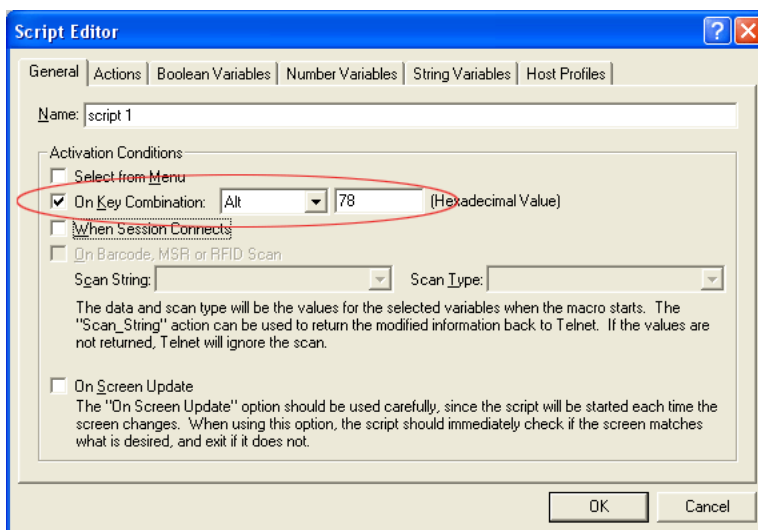
---

**NOTE** Use the Diagnostics utility to obtain the key value. Refer to *Using the Telnet Client Diagnostics Utility* on page 149 for more information.

---

**To configure the On Key Combination method:**

- 1 Select the General tab or Activate tab in the Script Editor.
- 2 Enable the **On Key Command** option.



**Figure 5-6.** On Key Combination

- 3 Use the drop-down menu and text box to assign a key combination to the script.

**When Session Connects**

This option causes the script to activate when the host profile it supports is activated.

If you use this option, it is strongly recommended that you limit the script to the appropriate host profiles. Since the script will be activated before any information appears on the emulation screen, you will need to have your script wait for the appropriate screen to appear before it does anything. You should not have more than one script set to start when a session begins because the first script started will prevent any other scripts from running while it waits for the initial screen.

Refer to *Selecting Host Profiles* on page 90 for more information.

### To configure the When Session Connects method:

- 1 Select the General tab or Activate tab in the Script Editor.
- 2 Enable the **When Session Connects** option.

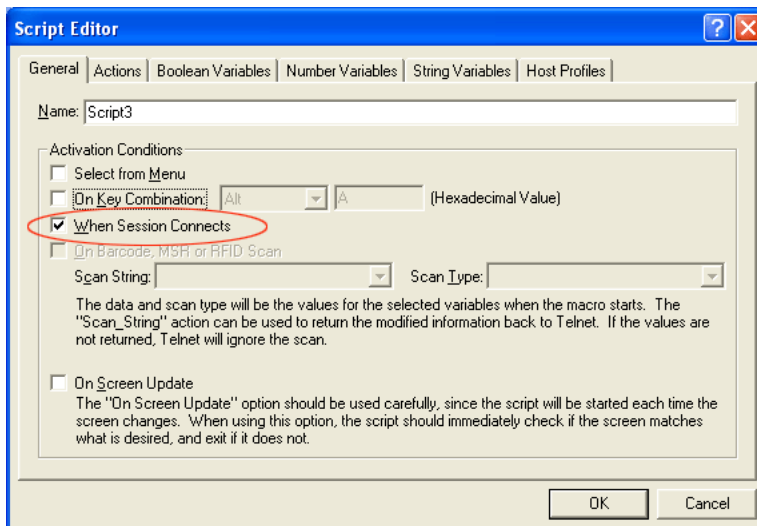


Figure 5-7. When Session Connects

- 3 Click **OK**.

### On Barcode, MSR or RFID Scan

This option allows the script to run with each barcode, MSR or RFID scan.

For detailed information on configuring scripts for barcode, MSR or RFID scan refer to the *Telnet Client Scripting Reference Guide*.

### To configure the On Barcode, MSR, or RFID Scan method:

- 1 Create the `Scan_String` and `Scan_Type` variables.

Once you create these variables, the **On Barcode, MSR or RFID Scan** options becomes available.

You will need to create these variables in the String Variables and Number Variables tabs. Refer to *Creating Variables* on page 88 for information on creating variables.



- 1 Select the General tab or Activate tab in the Script Editor.
- 2 Enable the **On Barcode, MSR, or RFID Scan** option.
- 3 From the drop-down menu, select the `Scan_String`.
- 4 From the drop-down menu select the `Scan_Type`.
- 5 Click `OK`.

### **On Screen Update**

This option will cause the script to be activated (if activation is allowed) every time the text on the emulation screen changes. This includes updates from the Telnet host or when the user presses a key and the key value is shown on the screen. It is recommended that you limit the host profiles that the script supports.

For detailed information on configuring scripts for on screen update execution refer to the *Telnet CE Client Scripting Reference Guide*.

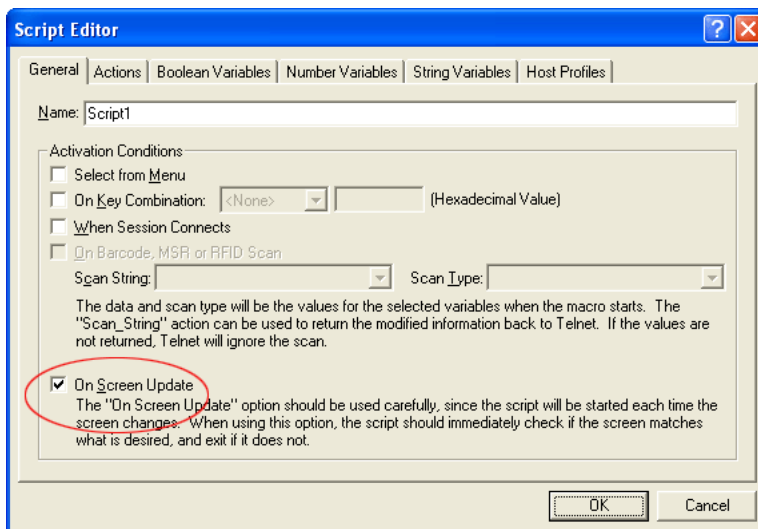
---

**NOTE** This option should be used carefully, since it can cause a script to be executed very frequently.

---

### **To configure the On Screen Update method:**

- 1 Select the General tab or Activate tab in the Script Editor
- 2 Enable the **On Screen Update** option.



**Figure 5-8.** Selecting the On Screen Update Method

3 Click OK.

## Creating the Script Code

Once you have named your script and selected an activation method, you can use the Actions tab in the Script Editor to build the script.

For detailed information and examples about building the script code refer to the *Telnet CE Client Scripting Reference Guide*.

## Creating Variables

There are three types of values recognized by scripting: booleans (TRUE or FALSE values only), numbers (integers), and strings. Every argument for every action is one of these three value types. Every action that returns a value returns one of these types. Variables provide a way to save the result of an action for use later as an argument for another command.

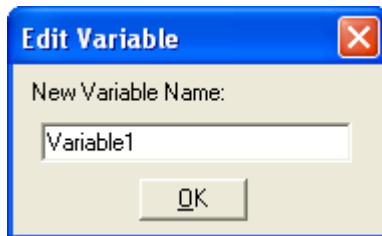
Variables can be created and edited under the appropriate Variable tab while editing the script. It is also possible to create new variables while editing an action.

When a script first starts, all the variables will have known values: boolean variables will be FALSE, number variables will be 0, and string variables will

be empty. One possible exception to this is when a script activates another script.

**To create a variable:**

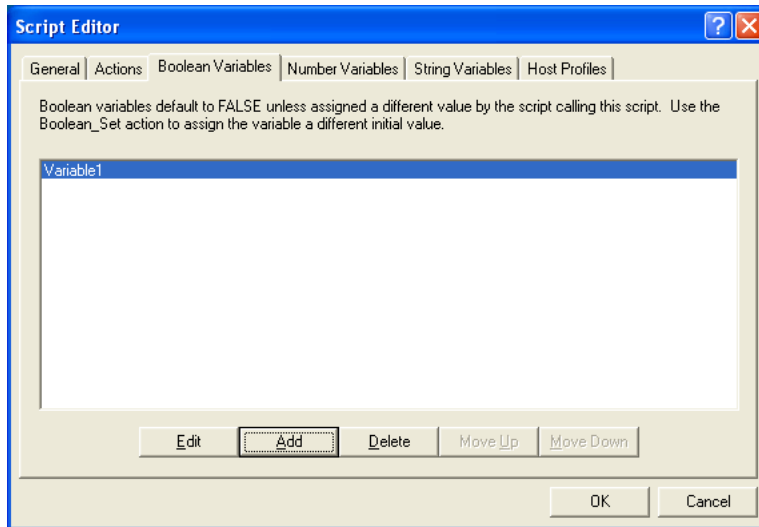
- 1 Determine which type of variable you want to create: boolean, number or string.
- 2 From the Script Editor, select the tab that corresponds with the type of variable you want to create.
- 3 Click **Add**.
- 4 In the *Edit Variable* dialog box, enter the name of the new variable.



**Figure 5-9.** Adding a New Variable

- 5 Click **OK**.

The new variable appears in the corresponding tab.



**Figure 5-10.** *New Variable*

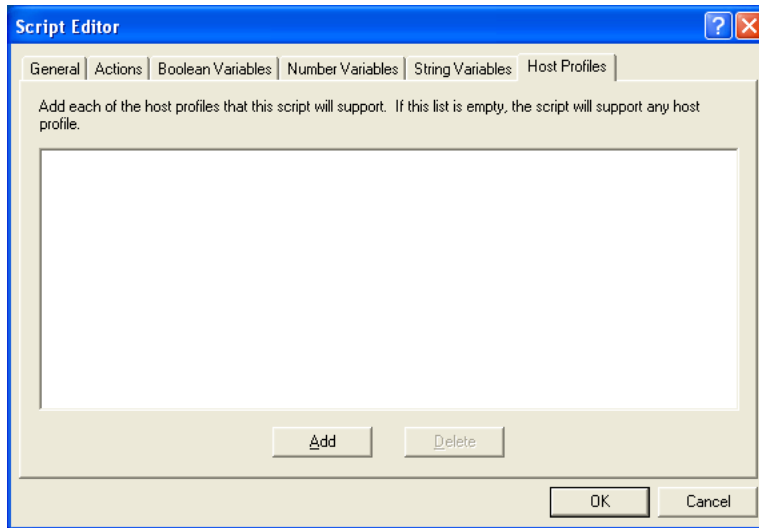
## Selecting Host Profiles

For each script, you can specify which host profiles will be supported by that script. You may select host profiles from the Host Profiles tab.

If the script is generated by script capturing, it is a good idea to limit that script to a host profile that was in use when the script was captured. The default - no host profile - allows the script to be run when any host profile is used.

### To select host profiles:

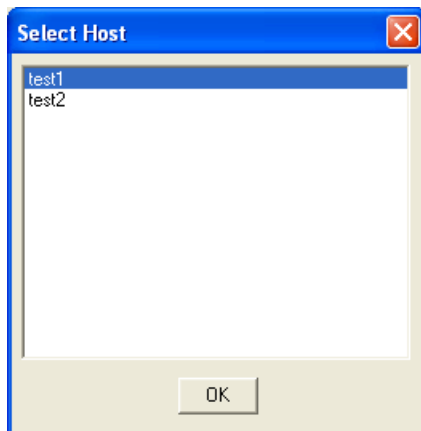
- 1 From the Script Editor, select the Host Profiles tab.



**Figure 5-11.** *Host Profiles Tab*

- 2 Click Add.

The *Select Host* dialog box opens.



**Figure 5-12.** *Selecting Host Profiles*

- 3 Select which host you want to use from the list of hosts.

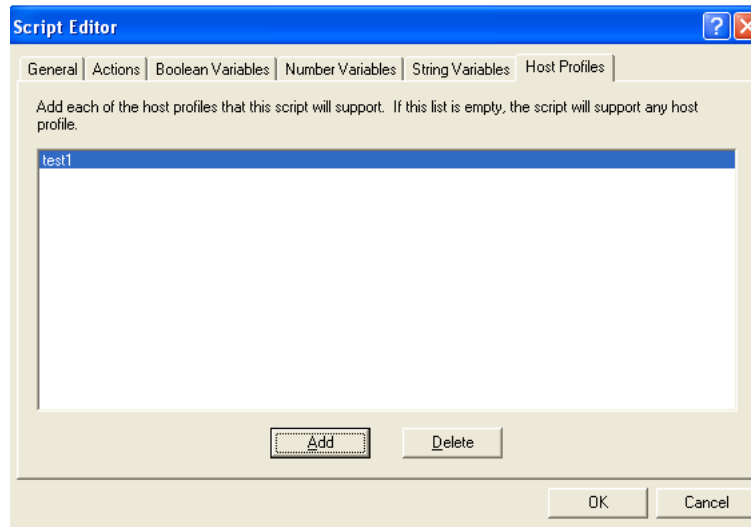
---

**NOTE** If you have not created any host profiles, this dialog box will be empty.

---

4 Click **OK**.

The host appears in the Host tab.



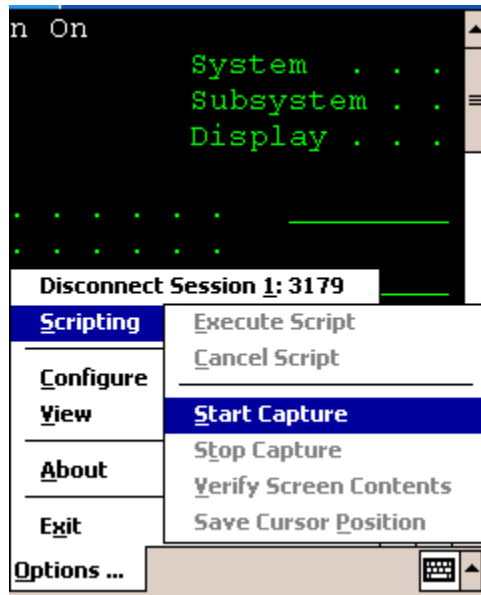
**Figure 5-13.** Selected Profile in Host Profiles Tab

## Performing Script Capturing

Script capturing is an easy way to generate a script that will automate doing something you can do manually. While script capturing is turned on, it will capture the key presses and mouse/pen cursor movements so they can be replayed with the script is activated.

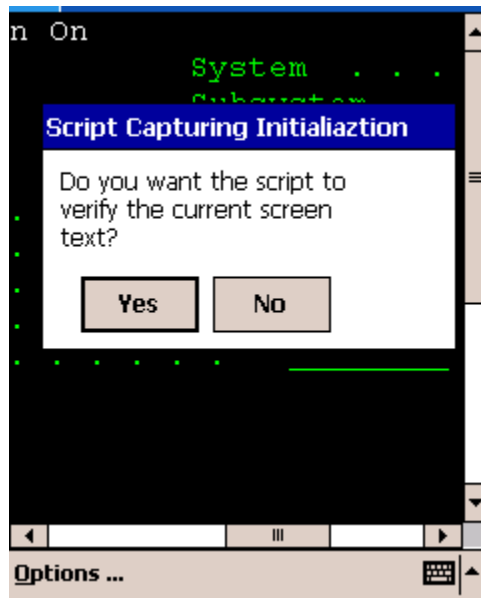
### To perform a script capture:

- 1 Position your mouse or cursor at the emulation screen you want to be at when the automated process starts.
- 2 From the **Term** or **Options** menu, select `Scripting > Start Capture`.



**Figure 5-14.** Starting Script Capture

- 3 At the prompt, select `Yes` to verify the current screen text.  
Select `No` if you do not want to verify the current screen text.



**Figure 5-15.** *Verifying the Current Screen Test*

Selecting `Yes` makes the captured script start with an `If_not` command that tells the script to exit if the correct screen is not currently shown. Unless you know that your script will only run from the correct screen (for example, a script that is run only when a session first starts, or a script called by another script), you should select `Yes`.

---

**NOTE** If you select `No`, click `Verify Screen Contents` and `Save Cursor Position` buttons when you start your script capture. This will cause your script to wait for Telnet to finish updating the screen before processing script actions.

---

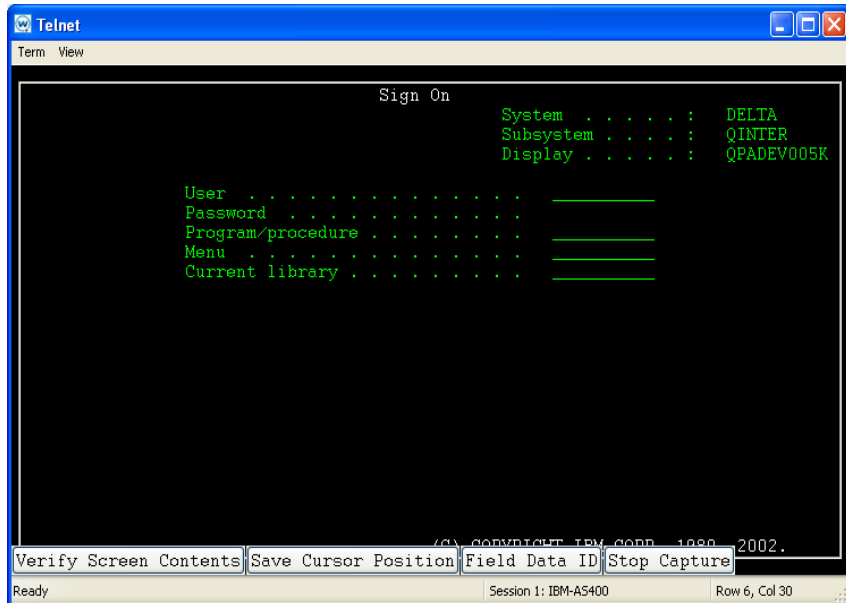
- 4 Perform any actions you want to include in the script.
- 5 Each time the screen changes, click `Verify Screen Contents` button.



---

**NOTE** Some devices may only display buttons labeled `Screen`, `Cursor`, `ID`, and `Stop`. The `Screen` button refers to the `Verify Screen Contents` button. The `Cursor` button refers to the `Save Cursor Position` button. The `ID` button refers to the `Field Data ID` button. The `Stop` button refers to the `Stop Capture` button.

---



**Figure 5-16.** *Verify Screen Contents and Save Cursor Position Buttons*

---

**NOTE** Clicking the `Verify Screen Contents` button will cause the generated script to pause and wait for the screen to be updated. The pauses are necessary because the scripts can run much faster than the interaction with the Telnet host.

---

- 6 When you are finished capturing the behaviors you want in the script, click `Stop Capture`.

Once you have captured a script, Script Editor opens. This allows you to name the script and select an activation method. You would also use the

Actions tab to add actions for any error condition that the user may encounter.

## Field Data ID Button

The Field Data ID feature allows you to use scripting to configure Field Data Identifiers. Field Data Identifiers assign a unique ID, such as a letter, to each field on the screen. Any time a barcode beginning with that ID is scanned, the information is automatically populated in the corresponding field. For detailed information and examples about the Field Data ID feature, refer to the *Telnet CE Client Scripting Reference Guide*.

## Editing Scripts

You can edit scripts that are created manually and scripts that are generated from the script capture option.

### To edit scripts:

- 1 Launch the Script Editor.
- 2 Select the script you want to edit from the Script Editor script list.
- 3 Click `Edit`.
- 4 Make the desired changes in the *Script Editor* configuration dialog box.
- 5 Click `OK` to save your changes.

Once you have completed editing the script you have two options:

- Export the script to a specified location using the `Export` button in the Script Editor. Refer to *Saving and Exporting Scripts* on page 98 for more information.
- Execute the script by launching the Telnet CE Client and performing the activation method you assigned to this script. Refer to *Executing Scripts* on page 100 for more information.

## Importing Scripts

You can use the import button in the Script Editor to import previously created scripts.

---

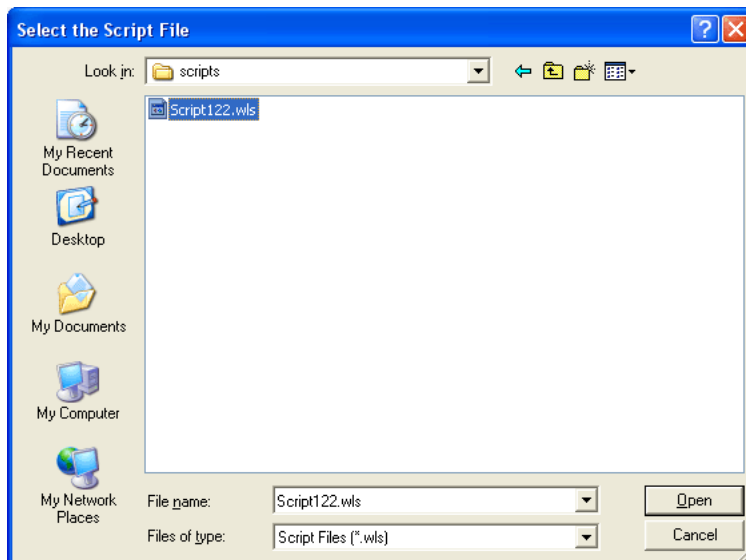
**NOTE** You can only import scripts that have been created using the Script Editor.

---

### To import a script:

- 1 From the Script Editor, click the `Import` button.

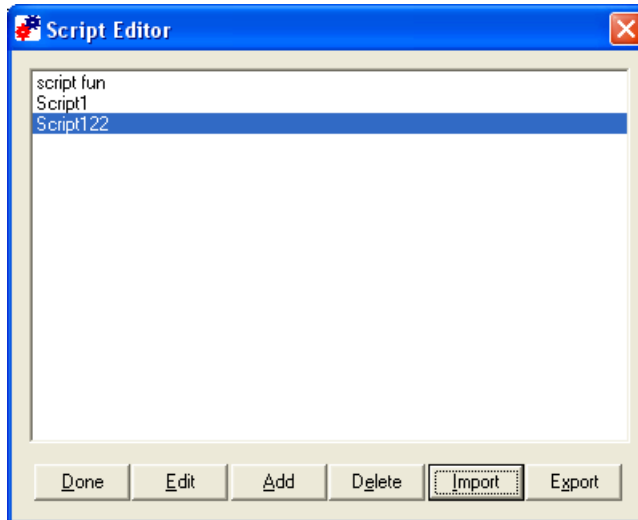
The *Select the Script File* dialog box opens.



**Figure 5-17.** *Importing a Script File*

- 2 Navigate to and select the script file.
- 3 Click `Open`.

The name of the file is imported into the Script Editor.



**Figure 5-18.** Imported Script File

Once you have imported the file, you can edit the script. Refer to *Editing Scripts* on page 96 for more information.

## Saving and Exporting Scripts

After you finish building a script, your script is automatically saved in the Script Editor. You can also export a script and save it in a specific location on the network.

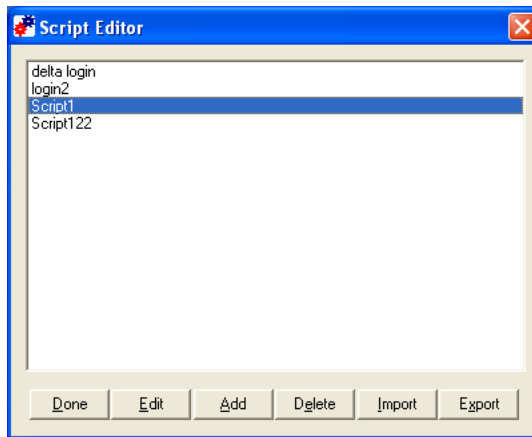
---

**NOTE** Scripts are saved as .wls files. Scripts can not be viewed outside the Script Editor and must be imported back in to the Script Editor to view or edit.

---

### To export a script:

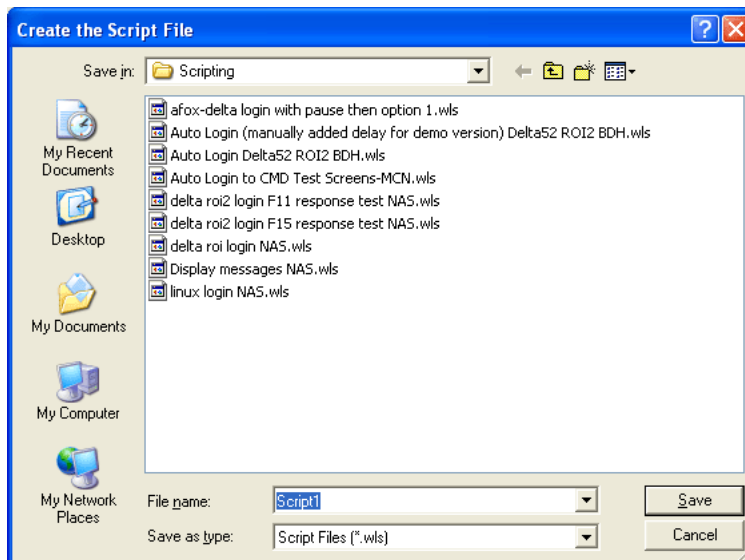
- 1 From the Script Editor script list, select which script you want to export.



**Figure 5-19.** *Selecting a Script to Export*

- 2 Click the `Export` button.

The *Create the Script File* dialog box opens.



**Figure 5-20.** *Exporting a Script*

- 3 Navigate to the location to which you want to export your script.

- 4 Click `Save`.

To view an exported script you will need to import that script into the Script Editor. Refer to *Importing Scripts* on page 97 for more information.

## Deploying Scripts

Scripts are deployed to the Telnet Client the next time the client syncs with the Avalanche Manager.

## Executing Scripts

When you create a script, you configure an activation method for that script. This section provides information about activating scripts using each of the following activation methods:

- Select from Menu
- On Key Combination
- When Session Connects
- On Barcode, MSR, or RFID Scan
- On Screen Update

For information on assigning an activation method to a script, refer to *Selecting the Activation Method* on page 83.

---

**NOTE** Screen captures may differ according to device type.

---

### Select from Menu

This option allows you to activate a script from the menu.

#### To activate a script using the **Select from Menu** option:

- 1 Launch the Telnet Client.
- 2 From the **Term** menu, select `Scripting > Execute Script` (Figure 5-21).

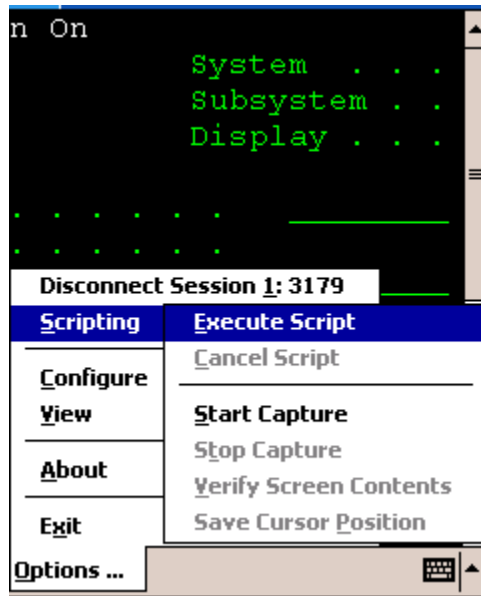


Figure 5-21. Executing a Script from the Menu

- 3 If more than one script is available for the current host profile, select which script you want to use from the list.

---

**NOTE** This option will not be available while a script is running for the current session or if the session is not connected.

---

## On Key Combination

This option lets you launch a script whenever a specified key combination is pressed (as long as it is currently possible for script to run).

### To execute a script on key combination:

- 1 Launch the Telnet Client.
- 2 Enter the key combination you assigned to execute the script.

## When Session Connects

This option causes the script to activate when the host profile it supports is activated.

**To execute when the session connects:**

- 1 Launch the Telnet Client.
- 2 From the **Term or Options** menu, select `Connect`.
- 3 Select to which host you want to connect.
- 4 Click `OK`.

The script will run upon connection.

**On Barcode, MSR, or RFID Scan**

When this option is assigned to a script, the script will activate with each barcode, MSR, or RFID scan.

**On Screen Update**

This option causes the script to be activated (if activation is allowed) every time the text on the emulation screen changes. This includes updates from the Telnet host or when the user presses a key and the key value is shown on the screen.



## Chapter 6: Keyboard Creator

This section provides the following information:

- Overview of Keyboard Creator
- Launching the Keyboard Creator
- Selecting Keyboard Files
- Creating Keyboards
- Importing Keyboard Graphics
- Creating and Configuring Keys
- Sizing and Positioning Keys and Rows
- Deploying the Keyboard to the Telnet CE Client

### Overview of Keyboard Creator

The Keyboard Creator allows you to create or modify the Telnet Client virtual keyboard.

Use the following steps to create a keyboard using Keyboard Creator:

- 1 Launch the Keyboard Creator.
- 2 Select the appropriate keyboard file.
- 3 Create a new keyboard.
- 4 Import a keyboard graphic, if desired.
- 5 Create and configure the keys of the keyboard.
- 6 Deploy the keyboard to the Telnet Client.

### Launching the Keyboard Creator

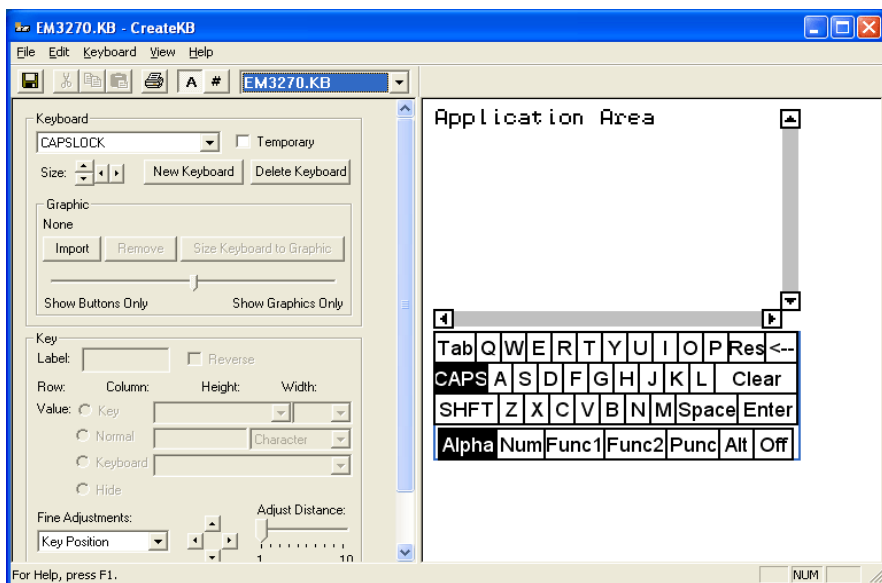
The Keyboard Creator is installed as part of the Telnet Client Avalanche software package.

**NOTE** The Keyboard Creator is only available in the Avalanche Telnet Client. You will not be able to access the Keyboard Builder from the ActiveSync install utility or any other third-party Telnet Client installation and configuration utilities.

**To launch from Avalanche:**

- 1 Select the Telnet Client software package in the Tree View of the Avalanche Manager.
- 2 Right-click the package and select Keyboard Creator.

The Keyboard Creator opens.



**Figure 6-1.** Launching the Keyboard Creator

## Selecting Keyboard Files

Keyboard files contain all the keyboards needed for a given emulation (5250, 3270, VT100, VT220, HP, or WEB). Use Table 6-1 to determine the name of the keyboard file that should be edited for a particular emulation.

Emulation	File Name
5250	EM5250.KB
3270	EM3270.KB
VT100, VT220	EMVT.KB
HP	EMHP.KB
WEB	EMWEB.KB

**Table 6-1:** *Emulation Types and File Names*

There are two additional keyboards:

- EMNONE.KB are the keyboards displayed when a session is not connected to a host.
- EMNUM.KB are the keyboards displayed for the Numeric keyboard option.

When the keyboard file is saved, a matching file with the .KBB extension will also be saved. This file is a binary representation of the keyboard file and will be used by the terminal to display the keyboards. (Telnet Client ignores the .KB files if they are present.)

### To select a keyboard file:

- 1 Determine the name of the Keyboard file you are creating.
- 2 Select the file type from the drop-down list.

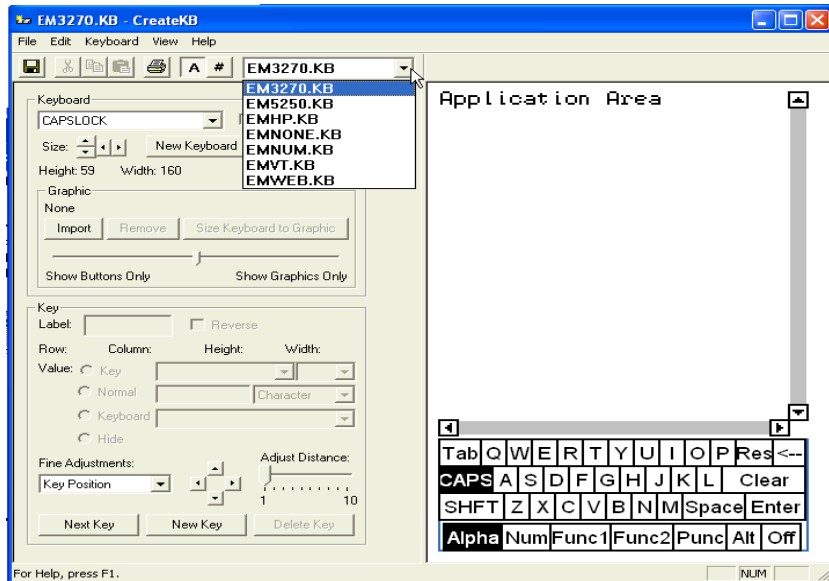


Figure 6-2. Selecting the File Type

## Creating Keyboards

There are two default keyboards: the default alpha keyboard and the default numeric keyboard. The default alpha keyboard is displayed by default. The default numeric keyboard is displayed when in a numeric field (5250 and 3270 only).

This section provides the following keyboard information:

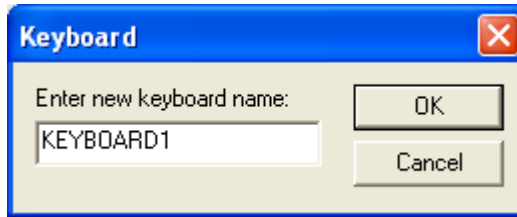
- Adding a new keyboard
- Sizing Keyboards
- Deleting Keyboards

### Adding a new keyboard

Multiple keyboards can be included in each keyboard file. The keyboards are linked together by shift keys (special keys which display another keyboard).

**To add a keyboard:**

- 1 Launch the Keyboard Creator.
- 2 Select **Keyboard > New Keyboard** from the menu.
- 3 Enter a new name for the keyboard.

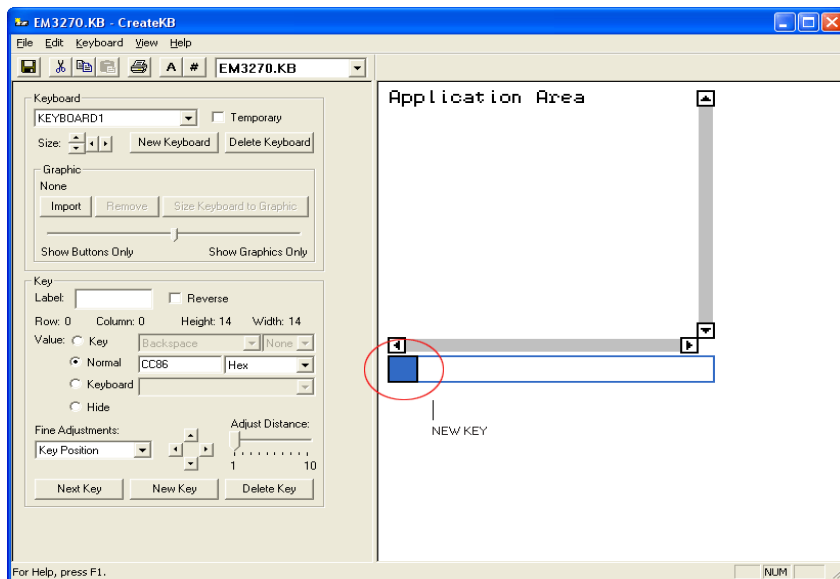


**Figure 6-3.** *Creating a New Keyboard*

---

**NOTE** Keyboard names must start with a letter, may only contain numbers or letters, and can only be 11 characters long.

---



**Figure 6-4.** *Creating a New Keyboard*

- 4 Use the Key configuration options to configure each key of the keyboard.

Refer to *Creating and Configuring Keys* on page 109 for more information.

## Sizing Keyboards

You can use the mouse to resize a keyboard. As you increase the size of the keyboard, the size of the application area will decrease.

### To resize the keyboard:

- 1 Mouse over the top border, right-side border, or the upper-right corner of the keyboard.
- 2 When the double-sided arrows appear, click and drag the keyboard to the desired size.

## Deleting Keyboards

When deleting a keyboard that has keys which connect to it, an option will be presented for dealing with any connections to the keyboard. Keys that are references to the keyboard being deleted can be deleted, set to an empty value or redirected to another keyboard.

### To delete a keyboard:

- 1 Select `Keyboard > Delete Keyboard` from the menu.
- 2 Select what action to take for referenced keys.

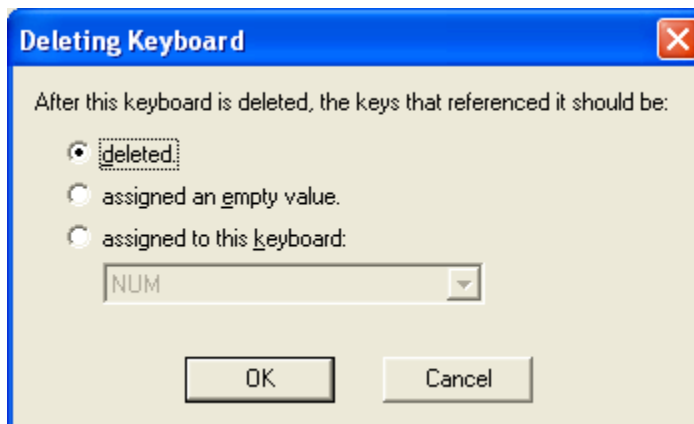


Figure 6-5. Deleting a Keyboard

## Importing Keyboard Graphics

The default keyboard draws the keys on the computer screen. However, you can import a graphic to be displayed instead of the created keys. An imported graphic will be embedded in the .KB and .KBB files, so you will not need to save the imported graphic file.

Key locations and values will still be used to determine which key the you clicked when you click on the keyboard graphic. You will need to create and position keys in the same position as the buttons on the imported graphic. Use the slider bar change how dark the graphic and buttons are while editing so that you can size and position the buttons correctly.

---

**NOTE** Be sure to label the buttons you create. If the mobile device is unable to use the bitmap image, the labeled buttons will still appear.

---

### To import a graphic:

- 1 In the Keyboard Creator, click `Import`.
- 2 Navigate to the location of the bitmap image you want to import.
- 3 Click `Open`.
- 4 Click the `Size Keyboard to Graphic` button to make the keyboard the same size as the imported graphic.
- 5 Use the slider bar to adjust the how dark and how light the graphics and buttons appear when editing.

## Creating and Configuring Keys

There are three types of keys that can be on a keyboard:

- Normal keys represent letters, numbers, or other characters in the emulation and can also represent special emulation specific function keys.
- Shift keys can point to any other keyboard in the current keyboard file.
- Hide keys hide the keyboard and allows an unobstructed view of the emulation screen.

This section provides the following information:

- Adding a new key
- Sizing and Positioning Keys and Rows
- Deleting Keys

### **Adding a new key**

You can add new keys to a keyboard and configure the key values and configure the following options:

- **Label.** Enter the text that will appear on the virtual key when it is displayed.
- **Reverse.** Enable this option for a key that indicates the active keyboard type.
- **Key Value.** Select from Key, Normal, Keyboard (shift), or Hide. Key values allow you to select emulation-specific actions to be assigned to the keys. The list of keys available will vary depending on the emulation type selected.

---

**NOTE** Normal key values can be displayed or entered as a character value (the actual character created by the keystroke is shown), a decimal value (for characters which cannot be shown), or a hexadecimal value (for scan codes of special function keys).

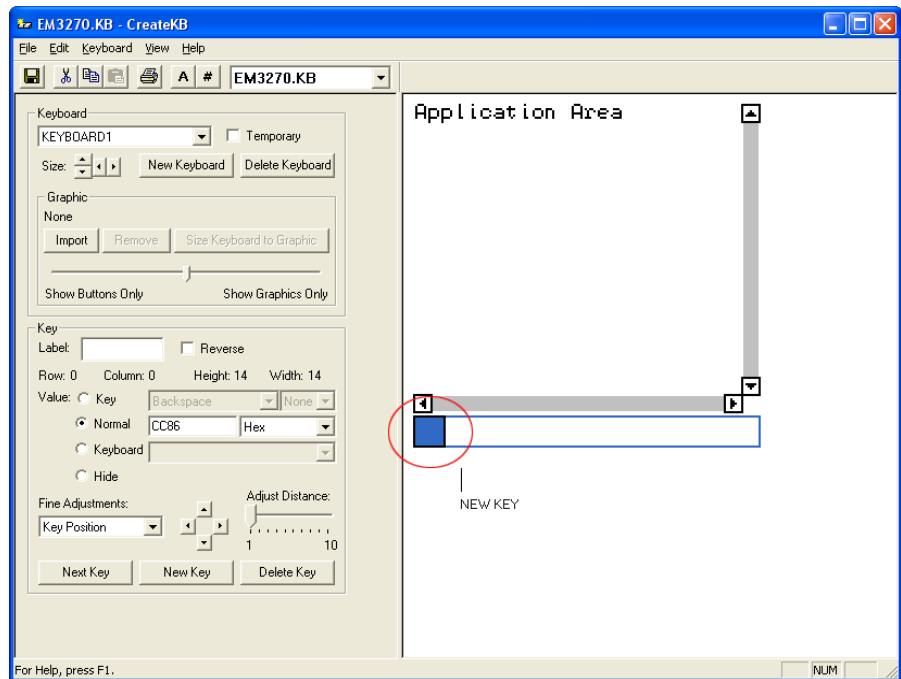
---

#### **To add a new key:**

- 1 Select `Keyboard > Add Key`.

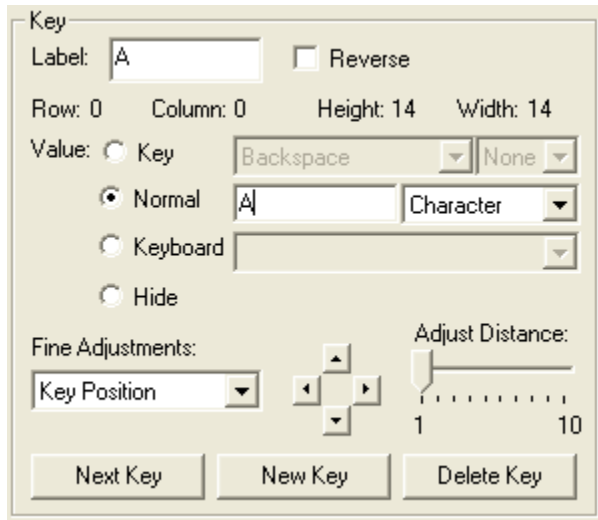
The new key will appear in the top left corner of the keyboard, or directly to the right of a selected key (if it will fit).





**Figure 6-6.** Adding a New Key

- 2 Modify the values for the key using the key configuration options.



**Figure 6-7.** *Configuring a New Key*

- 3 Repeat to create additional keys for the keyboard.

## Sizing and Positioning Keys and Rows

You can use the configuration options in the Key region of the Keyboard Creator to modify the size and position of the keys on the keyboard.

The Fine Adjustments drop-down menu allows you to select what object you want to modify:

- **Key Position.** Select this option to move a selected key on the keyboard. You can also adjust the key position by clicking on the key and dragging it to the desired position.
- **Row Position.** Select this option to move an entire row.
- **Keyboard Position.** Select this option to move all the keys on the keyboard.
- **Key Size.** Select this option to adjust the size of the key.

Once you select the object you want to modify, you can use the arrow buttons to position or size the keys and rows. The Adjust Distance slider

determines the distance that the arrow buttons move or adjust the keys or rows. You can use the slider to change the distance from 1-10 pixels.

**To position a key:**

- 1 Click `New Key`.
- 2 From the Fine Adjustments drop-down menu, select `Key Position`.
- 3 Use one of the following methods to move the key:
  - Use the arrow buttons to position the key in the desired location.
  - Drag and drop the key to the desired location.

**To position a row:**

- 1 Click a key in the row you want to position.
- 2 From the Fine Adjustments drop-down menu, select `Row Position`.
- 3 Use the arrow buttons to position the row in the desired location.

**To resize a key:**

- 1 Click `New Key` or select an existing key.
- 2 From the Fine Adjustments drop-down menu, select `Key Size`.
- 3 Use the arrows to adjust the size.

**Deleting Keys**

You can delete keys that you do not want from the keyboard.

**To delete a key:**

- 1 Select the key you want to delete.
- 2 Select `Keyboard > Remove Key`.

## Deploying the Keyboard to the Telnet CE Client

Once you have completed creating your keyboard and keys, click the `Save` icon to save your keyboard, and then exit the Keyboard Creator. Your Telnet CE Client will update with the new keyboard the next time the mobile device syncs with Avalanche Manager.



## Chapter 7: Resource Editor

This section provides the following information:

- Overview of Resource Editor
- Launching the Resource Editor
- Using the Resource Editor
- Deploying Files to the Telnet Client

### Overview of Resource Editor

The Resource Editor allows you to import sound and picture files that can be deployed to your mobile devices through Avalanche Manager.

Use the following steps to deploy sound and picture files to mobile devices:

- 1 Launch the Resource Editor.
- 2 Add bitmap and sound files.
- 3 Deploy bitmap and sound files to the Telnet Client.

### Launching the Resource Editor

The Resource Editor is installed as part of the Telnet Client Avalanche software package.

---

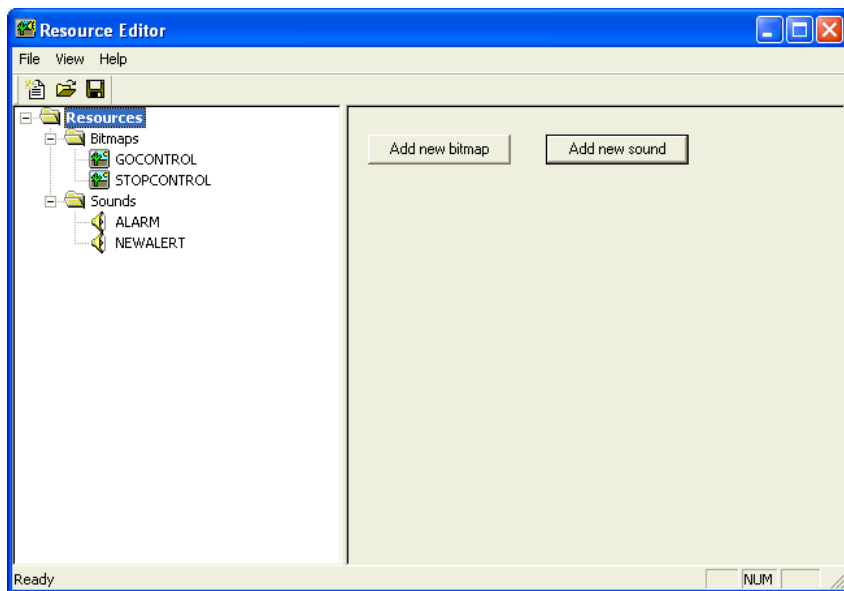
**NOTE** The Resource Editor is only available in the Avalanche Telnet Client. You will not be able to access the Resource Editor from the ActiveSync install utility or any other third-party Telnet Client installation and configuration utilities.

---

#### To launch from Avalanche:

- 1 Select the Telnet Client software package in the Tree View of the Avalanche Manager.
- 2 Right-click the package and select `Resource Editor`.

The Resource Editor opens.



**Figure 7-1.** *Launching the Resource Editor*

## Using the Resource Editor

There are two file types that can be imported into the Resource Editor: .bmp and .wav files. All files can be edited and removed as desired.

This section provides the following information:

- Adding a Bitmap
- Adding a Sound
- Playing Sounds
- Editing Files

### **Adding a Bitmap**

Any graphic file with a .bmp extension can be added to the Resource Editor.

**To add a bitmap:**

- 1 Launch the Resource Editor.
- 2 From the right pane of the Resource Editor, click `Add new bitmap`.

The *Open* dialog box appears.

- 3 Navigate to the desired file and click `Open`.

The file appears beneath the **Bitmaps** folder in the left pane of the Resource Editor.

**Adding a Sound**

Any sound file with a .wav extension can be added to the Resource Editor.

**To add a sound:**

- 1 Launch the Resource Editor.
- 2 From the right pane of the Resource Editor, click `Add new sound`.

The *Open* dialog box appears.

- 3 Navigate to the desired file and click `Open`.

The file appears beneath the **Sounds** folder in the left pane of the Resource Editor.

**Playing Sounds**

You can play your .wav files from the Resource Editor.

**To play a .wav file:**

- 1 Launch the Resource Editor.
- 2 In the left pane, expand the **Sounds** folder and select the desired file.
- 3 In the right pane of the Resource Editor, click `Play`.

The sound plays.

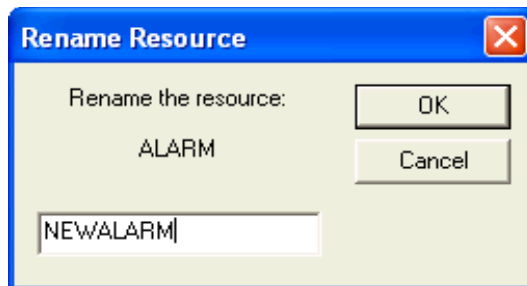
**Editing Files**

You can use the Resource Editor to rename or remove files.

**To rename files:**

- 1 Launch the Resource Editor.
- 2 In the left pane, expand the appropriate folder and select the desired file.
- 3 In the right pane of the Resource Editor, click `Rename`.

The *Rename Resource* dialog box appears.



**Figure 7-2.** *Rename Resource Dialog Box*

- 4 Enter the new file name in the available text box.
- 5 Click `OK`.

The new file name appears in the left pane of the Resource Editor.

**To remove files:**

- 1 Launch the Resource Editor.
- 2 In the left pane, expand the appropriate folder and select the desired file.
- 3 In the right pane of the Resource Editor, click `Remove`.

The *Resource Editor* dialog box appears.





**Figure 7-3.** *Resource Editor Dialog Box*

- 4 Click **Yes**.

The file is removed from the Resource Editor.

## Deploying Files to the Telnet Client

Once you have finished adding bitmap and sound files, click the **Save** icon to save your changes, and then exit the Resource Editor. Your Telnet Client will update with the new files the next time the mobile device syncs with Avalanche Manager.



## Chapter 8: Licensing

This section provides the following information:

- Overview of Licensing
- Types of Licenses
- Licensing Methods

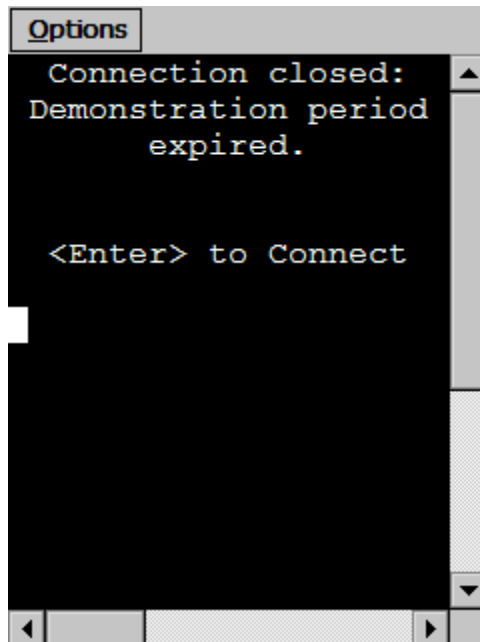
### Overview of Licensing

The Telnet Client requires a license for full functionality. You can use the Telnet Client without a license, but you will be limited to the demo version, which does not provide full Telnet Client functionality.

Telnet Client licensing is on a per-client basis, not on a per-connection basis. This means that a single license allows the Telnet Client to engage in the maximum number of Telnet sessions that the Telnet Client is configured to support (up to four concurrent sessions).

When the Telnet Client does not have a valid license, it operates in demo mode. When the Telnet Client is operating in demo mode, it will behave as followings:

- **Attempt to contact a license server.** Each time that you attempt to initiate a terminal emulation session, the Telnet Client will begin broadcasting in an attempt to locate a license server. At that point, you are prompted to either enter a license or to initiate the session in demo mode.
- **Prematurely disconnect emulation sessions.** While in demo mode, you may initiate terminal emulation sessions with hosts. However, each terminal emulation session that you initiate will automatically time out after one hour.



**Figure 8-1.** *Demonstration Period Expired*

## Authorization Methods

There are three ways to license (authorize) the Telnet Client:

- **Pre-licensing.** The Telnet Client may come pre-installed and pre-licensed on your mobile device. For pre-licensing information, please consult the Telnet Client reference guide for your mobile device manufacturer.
- **Manually.** You may manually input licensing information at the mobile device through the Telnet Client interface.
- **License Server.** You may use License Server to automatically provide Telnet Client licenses to the mobile devices on your network.

---

**NOTE** To obtain Telnet Client licenses, please contact Wavelink customer service. *Appendix D: Wavelink Contact Information* on page 267 provides Wavelink contact information.

---

## Types of Licenses

There are two types of Telnet Client licenses:

- Platform
- Maintenance

---

**NOTE** Maintenance licenses were added to the 5.0 version of the Telnet Client. Only platform licenses are available for 4.x Telnet Clients.

---

### About Platform Licenses

A platform license authorizes you to the version of the Telnet Client that you purchased and any builds associated with that version. For example, if you purchased a 5.0 Telnet Client license, then you are entitled to use 5.00-xx Telnet Client builds. If you want to use the features available in the 6.00-xx Telnet Client, then you must either buy a 6.0 platform license for your mobile devices, or you must purchase a maintenance license for your devices.

A platform license provides for minor upgrades and code changes, but does not allow major upgrades and updates to the Telnet Client.

Platform licenses do not expire, but they do not allow you to upgrade to a greater version of the Telnet Client.

### About Maintenance Licenses

A maintenance license allows you to upgrade your Telnet Client when new major versions of the Telnet Client become available. For example, a maintenance license allows you to upgrade from Telnet Client 5.x to Telnet Client 6.x.

Maintenance licenses are valid only through a specific date. After the expiration date, if you upgrade the Telnet Client, it will revert to operating in demo mode.

## Licensing Methods

This section provides the following information:

- Manually Licensing the Telnet Client
- Using License Server to License the Telnet Client

## Manually Licensing the Telnet Client

You may key in your authorization information manually through the Telnet Client interface.

### To manually configure a Telnet Client license:

- 1 Obtain the Telnet Client licensing information from Wavelink Corporation.
- 2 On the mobile device, launch the Telnet Client.
- 3 Attempt to establish a connection to a host.

---

**NOTE** For information about connecting to a host, see *Using the Telnet Client and Connecting to Hosts* on page 127.

---

If the Telnet Client has not attained a license, when you attempt to connect to a host, the *Authorizing Terminal* dialog box appears.

- 4 In the *Authorizing Terminal* dialog box, select **Add License**.

The *Authorization* dialog box appears.

- 5 In the **License Name** text box, type the name of the license.
- 6 In the **Serial #** text box, type the serial number for the license.
- 7 In the **Exp. Date** text box, type the expiration date of the license, in the format of MMDDYYYY.
- 8 In the **Code** text box, type the authorization code for the license.
- 9 In the **User #** text box, enter a user number.

---

**NOTE** The user number can be any number between 1 and the number of users (the limit) for which the license provides. Each Telnet Client should be configured with a unique user number.

---

**10** In the **Limit** text box, enter the user limit for the license.

**11** Click `Authorize`.

The license type appears in the **Platform** text box.

## Using License Server to License the Telnet Client

License Server is a Wavelink application that runs on a host system. The license server is responsible for supplying licenses to mobile devices that are using the Telnet Client.

---

**NOTE** The Telnet Client license server should not be confused with the Avalanche license server. Both are separate Wavelink applications.

---

---

**NOTE** For information about installing and using the Telnet license server, see *Appendix C: Using the Telnet Client License Server* on page 257.

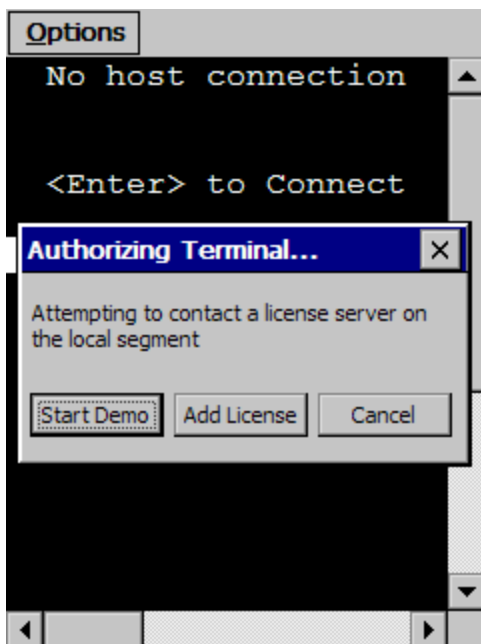
---

### Using a Local License Server

When you attempt to initiate a Telnet session with a host, if the Telnet Client is not already licensed, it will automatically attempt to obtain a license from a license server by using the following steps:

**1** The Telnet Client broadcasts a request for a license on the local IP network.

The *Authorizing Terminal* dialog box displays on the mobile device while the Telnet Client attempts to locate a license server.



**Figure 8-2.** *Authorizing Terminal Dialog Box*

- 2 Any license servers on the local IP network with an available license respond by offering a license.
- 3 The Telnet Client accepts the first license that it receives and sends back a reply to the license server.

The *Authorizing Terminal* dialog box on the mobile device indicates that a license has been obtained.

If no license server responds to the request for a license, then the *Authorizing Terminal* dialog box continues to display until you close the dialog box, elect to use a demo license, or elect to manually add a license.

### **Using a Remote or Specific License Server**

If the license server is on a remote IP network or you want to specify the license server from which the Telnet Client should request a license, you must configure the Telnet Client with the IP address of the license server.



---

**NOTE** For more information about configuring the IP address of the license server, see *Configuring License Server IP Address* on page 239.

---

When you attempt to initiate a Telnet session with a host, if the Telnet Client is not already licensed, it will automatically attempt to obtain a license from the specified license server using the following steps:

- 1 The Telnet Client sends a request for a license to the specified license server.

The *Authorizing Terminal* dialog box displays on the mobile device while the Telnet Client attempts to locate a license server.

- 2 The license server on the local IP network respond by sending the Telnet Client a license.
- 3 The Telnet Client accepts the first license that it receives and sends back a reply to the license server.

### Using the Demo License

If you cannot obtain a license for the Telnet Client, you may use the demonstration license.

The demonstration license automatically disconnects an active Telnet session after one hour.

#### To use the Telnet Client demo license:

- 1 Launch the Telnet Client.
- 2 Use the Telnet Client to initiate a Telnet session with a host.
- 3 The *Select Host* dialog box appears.

---

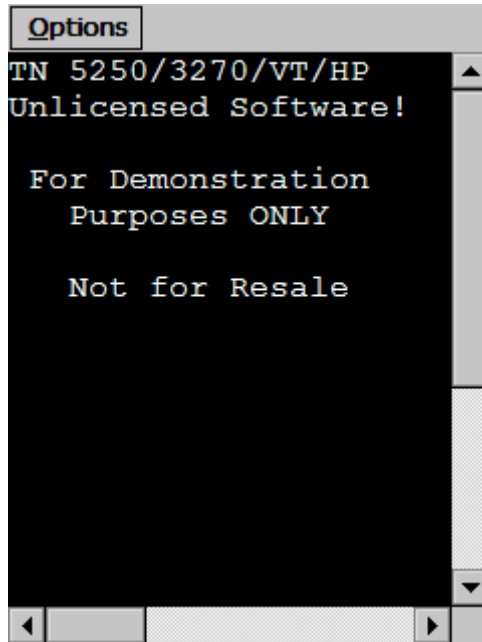
**NOTE** If you have configured the Telnet Client with only one host profile, the *Authorizing Terminal* dialog box appears.

---

- 4 In the *Select Host* dialog box, select the host with which you want to establish a Telnet session.

The *Authorizing Terminal* dialog box appears in the *Authorizing Terminal* dialog box, select `Start Demo`.

The Telnet Client uses the demonstration license and attempts to connect to the host that you selected. Before displaying the host emulation screen, the Telnet Client displays a screen that indicates that you are using a demonstration license.



**Figure 8-3.** *Telnet Client Running in Demonstration Mode*

## Chapter 9: Using the Telnet Client

This chapter provides the following information:

- Using the Telnet Client and Connecting to Hosts
- Working with Multiple Concurrent Telnet Sessions
- Using the Standard Virtual Emulation Keyboard
- Using Screen Panning
- Using ActiveText
- Using the Telnet Client Diagnostics Utility
- Using the Telnet Client Options Menu

### Using the Telnet Client and Connecting to Hosts

This section provides the following information:

- Launching the Telnet Client
- Initiating a Telnet Session
- Disconnecting a Telnet Session
- Exiting the Telnet Client

#### Launching the Telnet Client

Depending on the method that you used to install the Telnet Client, you will have different options for launching the Telnet Client.

If you installed the Telnet Client through Microsoft ActiveSync or another third-party application, then you will be able to launch the application from the Windows CE **Start** menu or from the desktop.

If you installed the Telnet Client through Avalanche Manager, then you will also be able to launch the Telnet Client from the Avalanche Enabler interface on the mobile device.

### Launching the Telnet Client From Windows

You can launch the Telnet Client from the **Programs** menu or, in some instances, from the desktop.

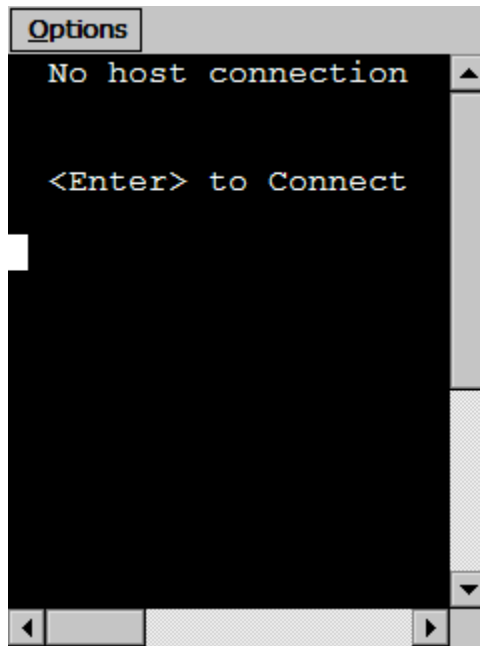
#### To launch the Telnet Client:

- 1 On the mobile device, access the Windows CE **Start** menu.
- 2 In the Windows CE **Start** menu, access the Programs group.
- 3 In the Programs folder, double-click the Telnet Client shortcut icon.



**Figure 9-1.** *Telnet Client Shortcut Icon*

The Telnet Client launches on the mobile device and displays the default screen.



**Figure 9-2.** *Telnet Client Default Screen*

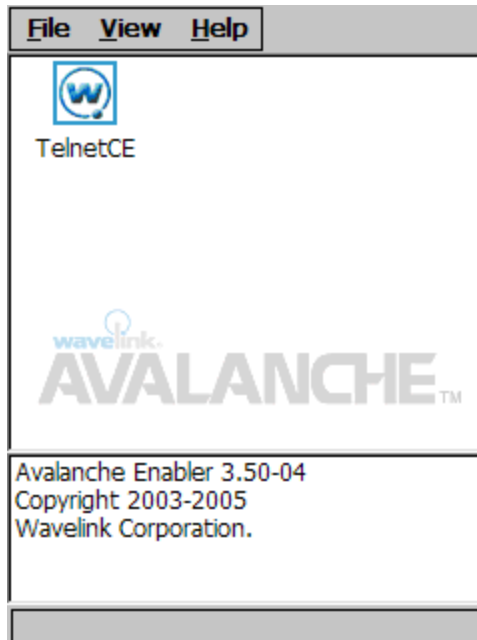
### **Launching the Telnet Client from Avalanche**

If you used Avalanche Manager to install the Telnet Client, then a shortcut icon for the Telnet Client appears in the Programs screen of the Avalanche Enabler.

#### **To launch the Telnet Client from the Avalanche Enabler:**

- 1 On the mobile device, launch the Avalanche Enabler.
- 2 If the Programs view is not available in the Avalanche Enabler, access the **View** menu and enable the Programs view.

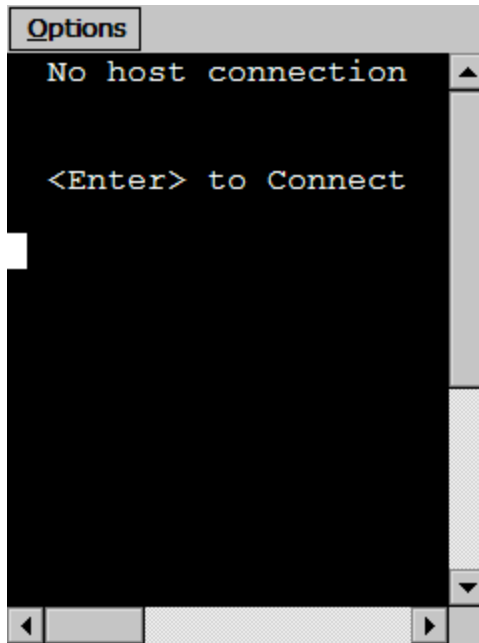
The Telnet Client shortcut icon appears in the Programs view of the Avalanche Enabler.



**Figure 9-3.** *Telnet Client Shortcut Icon in the Avalanche Enabler*

- 3** In the Programs view of the Avalanche Enabler, double-click the Telnet Client icon.

The Telnet Client launches on the mobile device and displays the default screen.



**Figure 9-4.** *Telnet Client Default Screen*

## Initiating a Telnet Session

Use the Telnet Client to initiate a Telnet session with any host for which you have configured a host profile.

---

**NOTE** For more information about host profiles and configuring host profiles for the Telnet Client, see *Chapter 3: Host Profiles* on page 29.

---

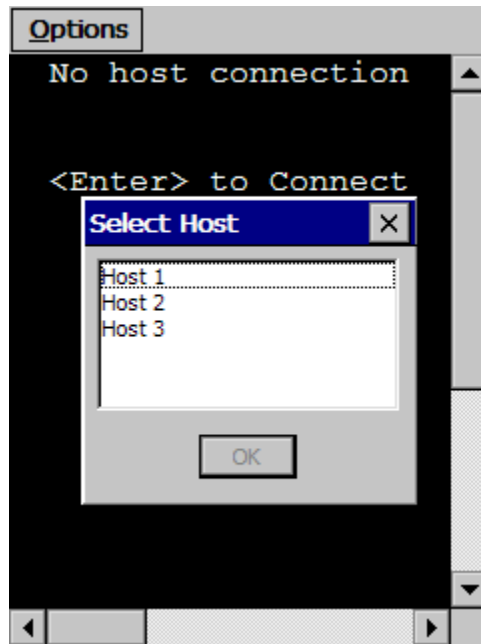
### To initiate a Telnet session with a host:

- 1 On the mobile device, launch the Telnet Client.

The Telnet Client launches and displays the default screen.

- 2 Press the `Enter` key.

The *Select Host* dialog box appears.



**Figure 9-5.** *Select Host Dialog Box*

---

**NOTE** If you have configured only one host profile for the Telnet Client, the *Select Host* dialog box does not appear. Instead, the Telnet Client automatically attempts to connect to the host for which you have configured the single host profile.

---

- 3 In the *Select Host* dialog box, select the host to which you want to connect.
- 4 Click **OK**.

The Telnet Client attempts to establish a Telnet session with the host.

---

**NOTE** If the client does not have a license, then the *Authorizing Terminal* dialog box appears. For more information about Telnet Client licensing, see *Chapter 8: Licensing* on page 119.

---

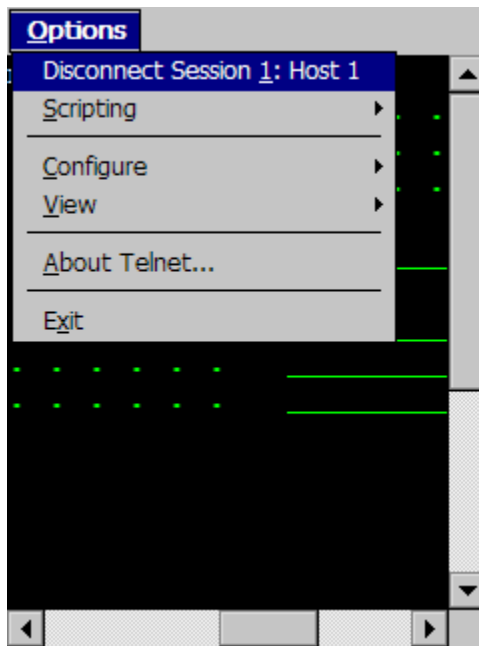


## Disconnecting a Telnet Session

Use the Telnet Client **Options** menu to disconnect from an active Telnet session.

**To disconnect from a Telnet session:**

- 1 Access the Telnet **Options** menu.
- 2 In the **Options** menu, select `Disconnect Session [n]-[name]`, where:
  - `<n>` is the session number that you want to disconnect, as displayed in the **Options** menu.
  - `<name>` is the name of the host from which you want to disconnect, as displayed in the **Options** menu.



**Figure 9-6.** *Disconnecting a Telnet Session*

When you make the selection, the session that you selected is terminated.

## Exiting the Telnet Client

You can use the Telnet Client **Options** menu to exit the Telnet Client. Depending on the configuration of the Telnet Client, you may be required to supply an exit password before you can exit the Telnet Client.

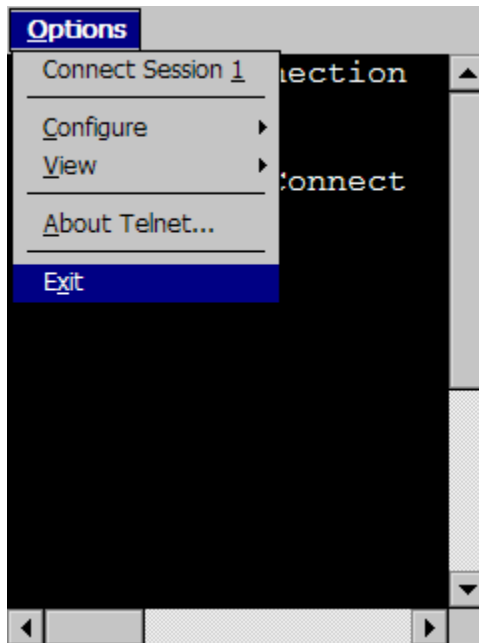
---

**NOTE** By default, the Telnet Client is not configured with an exit password. For more information about configuring an exit password for the Telnet Client, see *Configuring Passwords* on page 235.

---

### To exit and close the Telnet Client:

- 1 Access the Telnet Client **Options** menu.
- 2 In the Telnet Client **Options** menu, select `Exit`.



**Figure 9-7.** Exiting the Telnet Client

If you have configured the Telnet Client with an exit password, the *Input Password* dialog box appears.

If you have not configured an exit password, the Telnet Client closes.

- 3 In the *Input Password* dialog box, type the exit password.
- 4 Select **OK**.

The Telnet Client closes.

## Working with Multiple Concurrent Telnet Sessions

This section provides the following information:

- Overview of Multiple Concurrent Sessions
- Initiating an Additional Telnet Session
- Switching Between Active Telnet Sessions
- Disconnecting a Session

### Overview of Multiple Concurrent Sessions

The Telnet Client supports up to four concurrent Telnet sessions. These may include simultaneous sessions to the same host or to different hosts.

By default, the Telnet Client is configured to allow a user to engage in only one Telnet session. To provide for more than one active Telnet session, you must configure the Telnet Client to allow multiple concurrent sessions.

---

**NOTE** For information about configuring the Telnet Client to support multiple concurrent sessions, see *Configuring the Number of Concurrent Sessions* on page 237.

---

When the Telnet Client is configured to support multiple sessions, then multiple connection options appear in the Telnet Client **Options** menu.

### Initiating an Additional Telnet Session

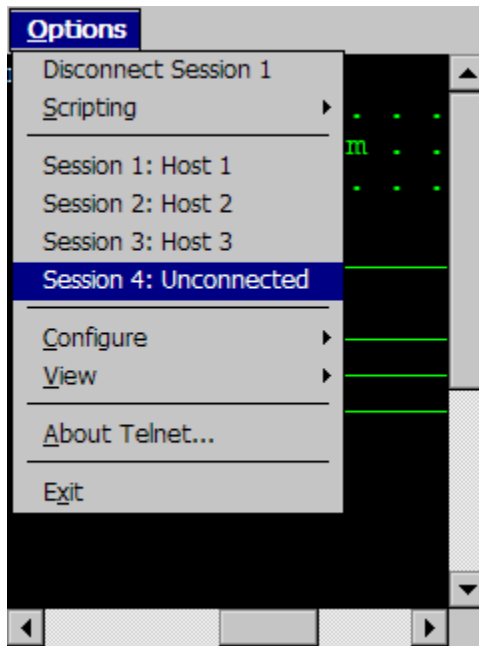
If you have configured the Telnet Client to allow multiple Telnet sessions and the Telnet Client is engaged in one or more Telnet sessions, you may initiate a new Telnet session from the **Options** menu.

**To initiate an additional Telnet session:**

- 1 Ensure that the Telnet Client is configured to allow multiple concurrent sessions.
- 2 Access the Telnet Client **Options** menu.

The **Options** menu displays the available sessions (between 1 and 4) and indicates which sessions are connected to a host and which are unconnected.

- 3 From the **Options** menu, select an unconnected session that you want to use to connect to the host.



**Figure 9-8.** Available Unconnected Telnet Session

The Telnet Client now displays the default screen. (The default screen prompts you to press `ENTER` to connect to a host.)

- 4 Press the `Enter` key.

The *Select Host* dialog box appears.

- 5 Use the *Select Host* dialog box to select the host with which you want to establish a Telnet session.
- 6 Select **OK**.

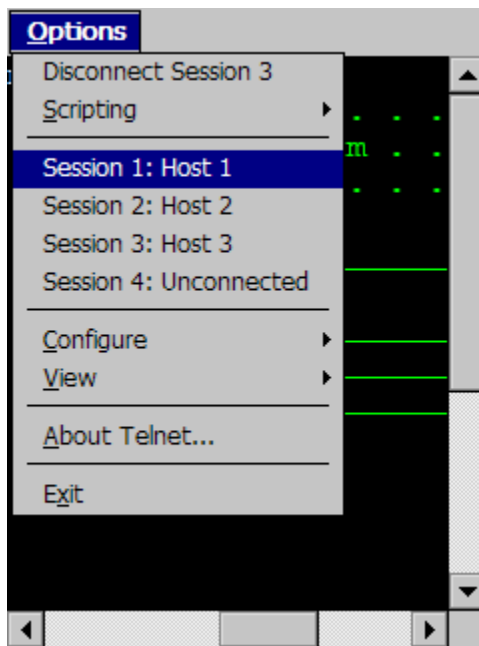
The Telnet Client attempts to connect to the host that you have selected.

### Switching Between Active Telnet Sessions

If the Telnet Client is engaged in more than one Telnet session, use the **Options** menu to switch between the sessions.

#### To switch between Telnet sessions:

- 1 In the Telnet Client, access the **Options** menu.
- 2 In the **Options** menu, select the active session that you want to view.



**Figure 9-9.** *Switching to a Different Telnet Session*

The Telnet Client switches the view to the Telnet session that you selected.

---

**NOTE** You can also use the `Next Sess` or `Prev Sess` keys in the virtual emulation keyboard to switch between sessions. For information about accessing the virtual emulation keyboard, see *Using the Standard Virtual Emulation Keyboard* on page 141.

---

### **Disconnecting a Session**

Use the **Options** menu to disconnect a session. You must switch to the session that you want to disconnect, before you can disconnect it.

#### **To disconnect a Telnet session:**

- 1** In the Telnet Client, access the **Options** menu.
- 2** From the list of sessions in the **Options** menu, select the session that you want to disconnect.

The Telnet Client switches the view to the session that you selected.

- 3** Access the **Options** menu again.
- 4** In the **Options** menu, select `Disconnect Session [n]`, where `[n]` is the session number that is currently active.

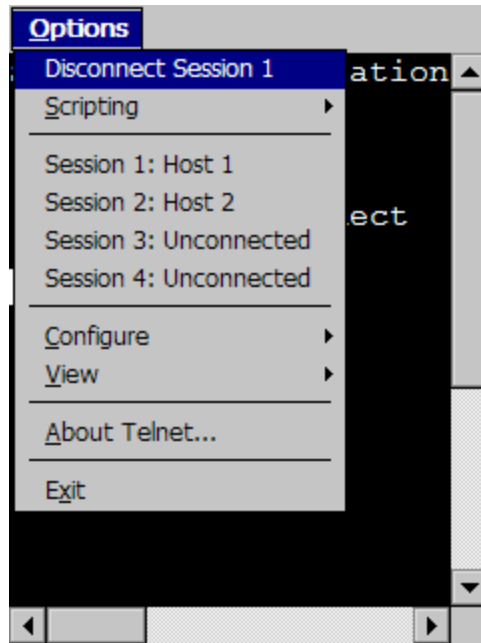


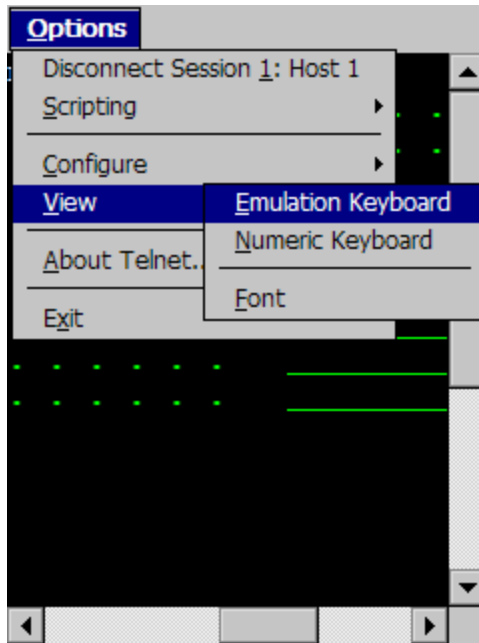
Figure 9-10. Disconnecting a Session

## Using the Standard Virtual Emulation Keyboard

The Telnet Client contains a default virtual emulation keyboard. You can access the keyboard through the Telnet Client **Options...** menu.

**To access the virtual emulation keyboard:**

- 1 Access the Telnet Client **Options...** menu.
- 2 Select `View > Emulation Keyboard`.



**Figure 9-11.** Accessing the Virtual Emulation Keyboard

The virtual emulation keyboard appears.

The type of emulation keyboard that displays is dependent on the emulation type of the current Telnet session. The VT/HP virtual emulation keyboard is different than the 5270/3270 virtual emulation keyboard. If there is not active session, then the basic virtual emulation keyboard appears.

### Using the Basic Virtual Emulation Keyboard

The following figure shows the basic Telnet Client virtual emulation keyboard.

TermConfig	Prog Info	Next Sess	
HostConfig		Prev Sess	
Keyclks	Quiet	Diags	Enter

**Figure 9-12.** Telnet Client Virtual Emulation Keyboard



The following list describes the function of the keys in the basic virtual emulation keyboard:

<b>TermConfig</b>	Allows you to access and configure the emulation parameters for a specific host profile.
<b>Prog Info</b>	Shows/hides the following information about the mobile device: <ul style="list-style-type: none"><li>• Telnet Client version information</li><li>• MAC address</li><li>• IP address</li><li>• ESSID</li></ul>
<b>Next Session</b>	Cycles to the next Telnet Client session.
<b>Host Config</b>	Allows you to access and configure the host profiles for the Telnet Client.
<b>Prev Session</b>	Cycles to the previous Telnet Client session.
<b>Keyclks</b>	Turns keyclicks on/off.
<b>Quiet</b>	Turns quiet mode on/off.
<b>Diags</b>	Allows you to access the Telnet Client diagnostic tools.
<b>Enter</b>	Connects the session.
<b>Close</b>	Disconnects the session. (Only available when the session is connected.)

### **Using the 5250/3270 Virtual Emulation Keyboard**

The following figure shows the Telnet Client virtual emulation keyboard for 5250/3270 emulation.

Tab	Q	W	E	R	T	Y	U	I	O	P	Res	<--
CAPS	A	S	D	F	G	H	J	K	L	FieldExit		
SHFT	Z	X	C	V	B	N	M	Space	Enter			
Alpha	Num	Func1	Func2	Punc	Alt	Off						

**Figure 9-13.** *Telnet Client 5250/3270 Virtual Emulation Keyboard*

The following list describes the function of the control keys that appear at the bottom of the virtual emulation keyboard:

- Alpha** Displays the alpha keys for 5250/3270 emulation, including:
- a - z
  - Tab, Caps Lock, Shft, Res, Backspace, FieldExit, Enter, Space, Alt
- Num** Displays the numeric keys for 5250/3270 emulation, including:
- 0 - 10
  - Mathematical symbols
  - Reset, Backspace, FieldExit, Enter, Arrow Keys
  - Tab, Shft, Space
- Func1** Displays the function keys for 5250/3270 emulation, including:
- F1 - F24
  - Roll Up, Roll Down, Enter

- Func2** Displays other function keys for 5250/3270 emulation, including:
- Dup, Print, Clear
  - Attn, Help, Home
  - Insert, Roll Up, Roll Down
  - Delete, SysRq, ErInp, Reset
- Punc** Displays punctuation characters for 5250/3270 emulation, including:
- Various punctuation and mathematical symbols
  - Reset, Field Exit, Enter
- Alt** Displays the basic virtual emulation keyboard. For information about the keys in the basic virtual emulation keyboard, see *Using the Basic Virtual Emulation Keyboard* on page 142.
- Off** Hides the virtual keyboard.

## Using the VT/HP Virtual Emulation Keyboard

The following figure shows the Telnet Client virtual emulation keyboard for VT/HP emulation.

Shft	Esc	q	w	e	r	t	y	u	i	o	p	<--
Ctrl	Tab	a	s	d	f	g	h	j	k	l	Enter	
Alt	Caps	z	x	c	v	b	n	m	Space		↑	
Alpha	Num	Func	Punc	Cfg	Off	←	→	↓				

**Figure 9-14.** Telnet Client VT/HP Virtual Emulation Keyboard

The following list provides information about the various control keys that appear at the bottom of the VT/HP virtual emulation keyboard.

<b>Alpha</b>	Displays the alpha keys for VT/HP emulation, including: <ul style="list-style-type: none"><li>• a - z</li><li>• Esc, Caps lock, Tab, Space, Enter, Backspace</li><li>• Shft, Ctl, Alt</li></ul>
<b>Num</b>	Display the numeric keyboard for VT/HP emulation, which contains the following keys: <ul style="list-style-type: none"><li>• 0 - 9</li><li>• Esc, Tab, Ins, Rem, Backspace, Enter, Space</li><li>• Shft</li></ul>
<b>Func</b>	Displays the function keys for VT/HP emulation, including: <ul style="list-style-type: none"><li>• F1 - F10</li><li>• Esc, Tab, Prev, Next, Find, Sel, Space, Backspace, Enter</li><li>• Shft, Ctrl, Alt</li></ul>
<b>Punc</b>	Display the punctuation keys for VT/HP emulation, including: <ul style="list-style-type: none"><li>• Punctuation Keys</li><li>• Backspace, enter, Space</li></ul>
<b>Cfg</b>	Display the basic virtual emulation keyboard. For information about the keys in the basic emulation keyboard, see <i>Using the Basic Virtual Emulation Keyboard</i> on page 142.

<b>Off</b>	Hides the virtual keyboard.
<b>Arrow Keys</b>	Moves the cursor in the direction of the arrow key that you press.

## Using the WEB Virtual Emulation Keyboard

The following figure shows the Telnet Client virtual emulation keyboard for WEB emulation.

Back	Fwd	Stop	Refresh	Home
Prev Sess		Next Sess		Close
Key Clicks		Quiet	Info	Diags
Alpha	Num	Func	Punc	Cfg
		Off	←	→
				↓

**Figure 9-15.** *Telnet Client WEB Virtual Emulation Keyboard*

The following list describes the function of the keys in the WEB virtual emulation keyboard.

<b>Back</b>	Returns the browser to the previous web page.
<b>Fwd</b>	Returns to the screen displayed before <b>Back</b> was selected.
<b>Stop</b>	Stops the web page from loading.
<b>Refresh</b>	Reloads the current web page.
<b>Home</b>	Returns the browser to the specified home page.
<b>Prev Sess</b>	Cycles to the previous Telnet Client session.
<b>Next Sess</b>	Cycles to the next Telnet Client session.
<b>Close</b>	Disconnects the session. (Only available when the session is connected.)
<b>Key Clicks</b>	Turns key clicks on/off
<b>Quiet</b>	Turns quiet mode on/off.

<b>Info</b>	<p>Shows/hides the following information about the mobile device:</p> <ul style="list-style-type: none"><li>• Telnet Client version information</li><li>• MAC address</li><li>• IP address</li><li>• ESSID</li></ul>
<b>Diags</b>	<p>Allows you to access the Telnet Client diagnostic tools.</p>
<b>Alpha</b>	<p>Displays the alpha keys for WEB emulation, including:</p> <ul style="list-style-type: none"><li>• a-z</li><li>• Shift, Ctl, Alt</li><li>• Esc, Tab, Caps, Enter, Space</li></ul>
<b>Num</b>	<p>Displays the numeric keyboard for WEB emulation, including:</p> <ul style="list-style-type: none"><li>• 0-9</li><li>• Shft</li><li>• Esc, Tab, Ins, Enter, Space</li></ul>
<b>Func</b>	<p>Displays the function keys for WEB emulation, including:</p> <ul style="list-style-type: none"><li>• F1-F24</li></ul>
<b>Punc</b>	<p>Displays the punctuation keys for WEB emulation, including:</p> <ul style="list-style-type: none"><li>• Punctuation keys</li><li>• Enter, Space</li></ul>
<b>Cfg</b>	<p>Display the virtual emulation keyboard.</p>

---

<b>Off</b>	Hides the virtual keyboard.
<b>Arrow Keys</b>	Moves the web page up and down or from side to side.

## Using Screen Panning

By default, the screen panning feature of the Telnet Client is enabled.

Screen panning feature of the Telnet Client allows a user to use the stylus to move around an emulation screen. When screen panning is enabled, a user can tap-and-drag the stylus and scroll across the emulation screen.

Screen panning has two modes of operation:

- **Standard.** By default, standard screen panning is enabled on the Telnet Client. When standard screen panning is enabled, the screen scrolls in the direction that the user drags the stylus across the screen. Standard screen panning simulates the effect of dragging the display of the mobile device over the emulation screen.
- **Reversed.** When reversed screen panning is enabled, the screen scrolls in the opposite direction that the user drags the stylus. Reverse screen panning simulates the effect of dragging the emulation screen beneath a fixed view port (that is, mobile device display).

---

**NOTE** For information about configuring screen panning, see *Configuring Screen Panning* on page 244.

---

## Using ActiveText

By default, the ActiveText feature of the Telnet Client is enabled.

ActiveText allows the Telnet Client to identify menu items and functions in an emulation screen and convert them to interactive objects that a user can double-click to execute.

When a string of text is turned into ActiveText, a user can perform the following actions on the ActiveText object:

- **Single-click.** A single click highlights the string of text and indicates that it has become an `ActiveText` object.
- **Double-click.** A double-click executes the menu item or the function that has been converted to an `ActiveText` object.

You can configure the Telnet Client to recognize two types of text strings that will be converted to `ActiveText` objects:

- Simple number menu item
- AS/400-style function key

---

**NOTE** For information about configuring `ActiveText`, see *Configuring ActiveText* on page 246.

---

### **Simple Number Menu Item**

The Telnet Client can recognize numbered options in a menu and convert them to an `ActiveText` object.

The Telnet Client recognizes a string of characters in the following list as a simple number menu item:

- A beginning of line or a space
- A number (a string of digits)
- A period (‘.’)
- A space
- A non-space character

For example, the Telnet Client would convert the menu item `90. Sign Off` in an emulation to `ActiveText`. The user could then double-click the `ActiveText` to invoke the `90. Sign Off` menu option.

### **AS/400-Style Function Key**

The Telnet Client can recognize AS/400-style function key commands in an emulation screen.



The Telnet Client recognizes the following string of characters as an AS/400-/style function key:

- A beginning of line or a space
- The character 'F'
- A number (string of digits)
- An equal-to character ('=')
- A non-space character

For example, the Telnet Client would convert the function key command `F3=Exit` to `ActiveText`. The user could then double-click the `ActiveText` to invoke the `F3=Exit` command.

## Using the Telnet Client Diagnostics Utility

The Telnet Client diagnostics utility allows you to perform the following tasks:

- Capture scan codes for external keyboard character sequences
- Perform a scan test
- Capture scan codes for the Windows virtual keyboard

### Accessing the Telnet Client Diagnostics Utility

Use the Telnet Client virtual keyboard to access the diagnostics utility.

**To access the diagnostics utility:**

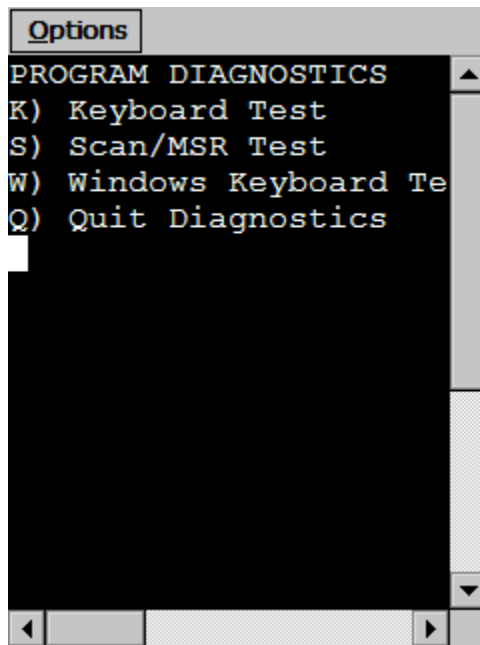
- 1 In the Telnet Client, access the virtual emulation keyboard.
- 2 In the virtual keyboard, click `Diags`.

---

**NOTE** `Diags` appears in the basic virtual emulation keyboard. For VT/HP emulation, `Diags` appears in the `Cfg` display of the virtual keyboard. For 5250/3270 emulation, `Diags` appears in the `Alt` display of the virtual keyboard.

---

The *Program Diagnostics* screen appears in the Telnet Client.



**Figure 9-16.** *Telnet Client Diagnostics Utility*

**3** Select one of the options in the Program Diagnostics screen:

- Press **K** to perform a keyboard test, which allows you to obtain scan codes for the external keyboard and the Telnet Client virtual keyboard.
- Press **S** to perform a scan test, which allows you to determine the type of barcode for a scan
- Press **W** to perform a Windows keyboard test, which allows you to obtain scan codes for the Windows virtual keyboard.
- Press **Q** to quick the diagnostics utility.

### **Performing a Keyboard Test**

Use the Telnet Client to obtain scan codes for the external keyboard and the Telnet Client virtual keyboard.

**To perform a keyboard test:**

- 1 Ensure that you have an active VT/HP or 5250/3270 Telnet session.

---

**NOTE** An active session is required to test the Telnet Client virtual keyboard. The virtual keyboard displays keys based on the current Telnet session type.

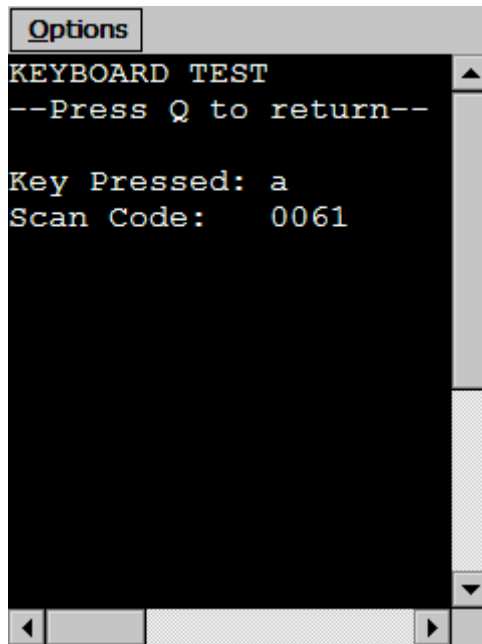
---

- 2 Use the Telnet Client virtual keyboard to access the *Program Diagnostics* screen.
- 3 Press  $\kappa$  for Keyboard Test.

The *Keyboard Test* screen appears.

- 4 Use the external keyboard or the virtual keyboard to submit a character sequence to the Telnet Client.

The Telnet Client displays the scan code for the character sequence.



**Figure 9-17.** *Performing a Keyboard Test*

- 5 Press **Q** to exit the *Keyboard Test* screen.
- 6 Press **Q** to exit the Telnet Client diagnostics utility.

### **Performing a Scan Test**

Use the Telnet Client diagnostics utility to perform a scan test. A scan test allows you to verify the type and value of scanned data. The scan test utility does not process any scan handlers, scan identifiers, or pre- or post-amble strings. However, scan identifiers that you have configured are added to the scan.

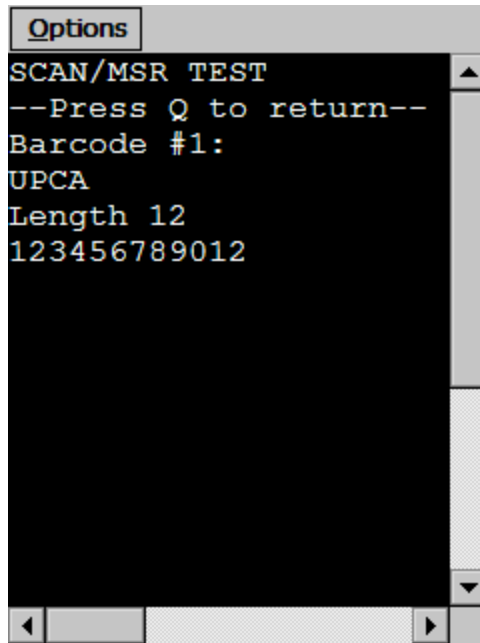
#### **To use the diagnostics utility to perform a scan test:**

- 1 In the Telnet Client, access the diagnostics utility.  

The *Program Diagnostics* screen appears.
- 2 Select **S** for Scan/MSR Test.  

The *Scan/MSR Test* screen appears.
- 3 Use the scanner on the mobile device to perform a test scan.  

The *Scan/MSR Test* screen displays the results of the scan.



**Figure 9-18.** *Performing a Scan Test*

- 4 Press **Q** to close the *Scan/MSR Test* screen.

## **Performing a Windows Keyboard Test**

Use the Telnet Client diagnostics utility to obtain scan codes for the Windows virtual keyboard.

### **To use the diagnostics utility to obtain Windows scan codes:**

- 1 In the Telnet Client, access the diagnostics utility.

The *Program Diagnostics* screen appears.

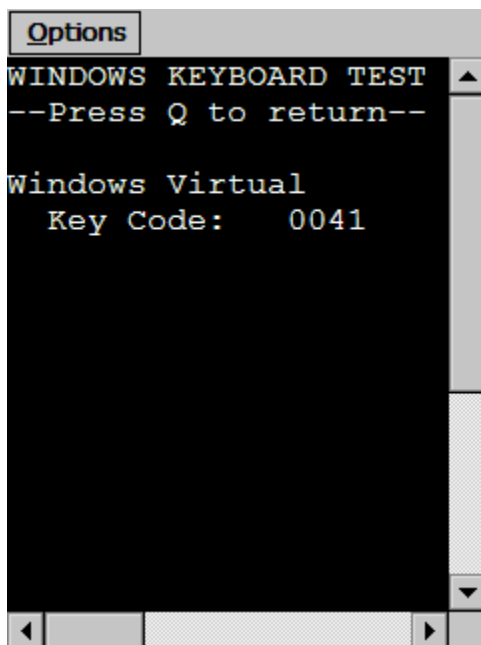
- 2 Select **w** for Windows Keyboard Test.

The *Windows Keyboard Test* screen appears.

- 3 Access the Windows virtual keyboard.

- 4 Select a character sequence in the Windows virtual keyboard.

The diagnostics utility displays the scan code for the character sequence that you submitted to the Telnet Client.



**Figure 9-19.** *Performing a Windows Keyboard Test*

- 5 Press `Q` to exit the *Windows Keyboard Test* screen.
- 6 Press `Q` to exit the diagnostics utility.

## Using the Telnet Client Options Menu

This section provides a description of each option in the Telnet Client **Options** menu.

- |                               |  |
|-------------------------------|--|
| <b>Connect Session [n]</b>    | Select this option to use the current session to initiate a Telnet connection with a host, where [n] is the session number that is currently active. |
| <b>Disconnect Session [n]</b> | Select this option to disconnect the current session, where [n] is the session number that is currently active.                                      |

---

<b>Session [n] - [name]unconnected</b>	Select this option to switch between sessions, where: <ul style="list-style-type: none"><li>• [n] indicates the session number</li><li>• [name] indicates that the session is currently connected to [name] host</li><li>• unconnected is a constant that indicates that the session is not currently in use</li></ul>
<b>Web &gt; Back</b>	Select this option to return the browser to the previous web page.
<b>Web &gt; Forward</b>	Select this option to return to the screen displayed before <code>Back</code> was selected.
<b>Web &gt; Stop</b>	Select this option to stop the web page from loading.
<b>Web &gt; Refresh</b>	Select this option to reload the current web page.
<b>Web &gt; Home</b>	Select this option to return the browser to the specified home page.
<b>Web &gt; Text Size</b>	Select this option to change the text size. The available options are: <ul style="list-style-type: none"><li>• Largest</li><li>• Larger</li><li>• Medium</li><li>• Smaller</li><li>• Smallest</li></ul>
<b>Scripting &gt; Execute Script</b>	XXX
<b>Scripting &gt; Cancel Script</b>	XXX
<b>Scripting &gt; Start Capture</b>	XXX
<b>Scripting &gt; Stop Capture</b>	XXX

---

<b>Scripting &gt; Verify Screen Contents</b>	XXX
<b>Scripting &gt; Save Cursor Position</b>	XXX
<b>Configure &gt; Host Profiles</b>	Select this option to configure host profiles for the Telnet Client.
<b>Configure &gt; Emulation</b>	Select this option to configure emulation parameters for the Telnet Client.
<b>Configure &gt; Scripting</b>	Select this option to edit scripts for the Telnet Client.
<b>Configure &gt; Authorization</b>	Select this option to configure licensing for the Telnet Client.
<b>Configure &gt; Localization</b>	Select this option to configure localization for the Telnet Client.
<b>Configure &gt; Resources</b>	Select this option to access the Resource Editor.
<b>View &gt; Emulation Keyboard</b>	Shows/hides the virtual emulation keyboard.
<b>View &gt; Numeric Keyboard</b>	Shows/hides the numeric keyboard.
<b>View &gt; Font</b>	Displays the font settings for the Telnet session. Use the Font tab in the dialog box to modify the font settings for the Telnet session.
<b>About Telnet...</b>	Displays the <i>About</i> window, which provides information about the Telnet Client.
<b>Exit</b>	Select this option to exit and close the Telnet Client. Depending on the configuration of the Telnet Client, you may need to supply an exit password.



## Chapter 10: Industrial Browser (WEB Emulation)

This chapter provides information about using and developing for the Telnet Client Industrial Browser. This chapter includes the following information:

- Overview of the Industrial Browser
- Licensing
- Industrial Browser Host Profile Settings
- Using the Industrial Browser
- Developing Web Pages for the Industrial Browser

### Overview of the Industrial Browser

Wavelink Telnet Client includes an Industrial Browser interface that gives you the ability to access web-based applications from a mobile device. The Industrial Browser supports PocketPC 2003, Windows Mobile 5.0, Windows 2000/XP, and Windows CE .NET 4.2/5.0.

---

**NOTE** The Industrial Browser is included in Telnet Client 6.0 and later versions.

---

### Licensing

The Telnet Client Industrial Browser requires a license for full functionality. There are two ways to license Telnet Client Industrial Browser:

- If you do not currently have a Telnet Maintenance license, you can purchase a Telnet Client 6.0 Standalone Browser license. (A separate Browser Maintenance license is also available.)
- If you currently have a Telnet Maintenance license, you can purchase an Industrial Browser add-on license. (Browser Maintenance is included.)

---

**NOTE** For more information on licensing, see *Chapter 8: Licensing* on page 119

---

## Industrial Browser Host Profile Settings

This section describes the parameters of each tab used to configure WEB emulation settings in the *Host Profiles* dialog box.

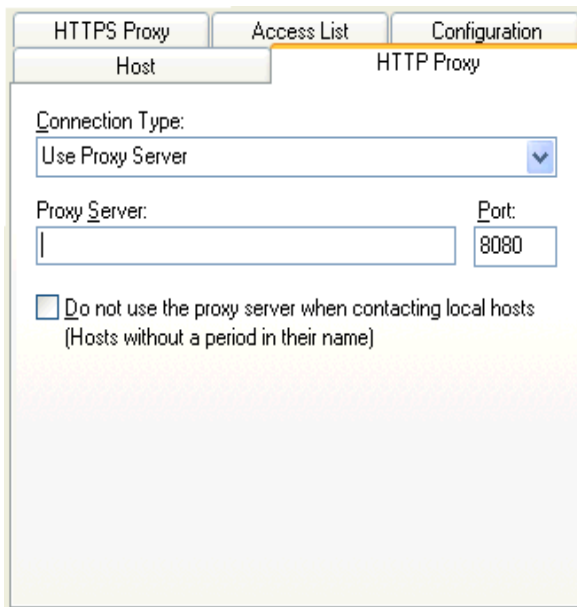
---

**NOTE** For more information on Host Profile Settings, see “Host Profiles” on page 29.

---

### HTTP Proxy Tab

Use the HTTP Proxy tab to configure proxy connections for WEB emulation.



The screenshot shows a dialog box with three tabs: "HTTPS Proxy", "Access List", and "Configuration". The "Configuration" tab is active, and within it, the "HTTP Proxy" sub-tab is selected. The "Host" sub-tab is also visible. The "HTTP Proxy" section contains the following fields:

- Connection Type:** A dropdown menu with "Use Proxy Server" selected.
- Proxy Server:** A text input field.
- Port:** A text input field with "8080" entered.
- Do not use the proxy server when contacting local hosts**  
(Hosts without a period in their name)

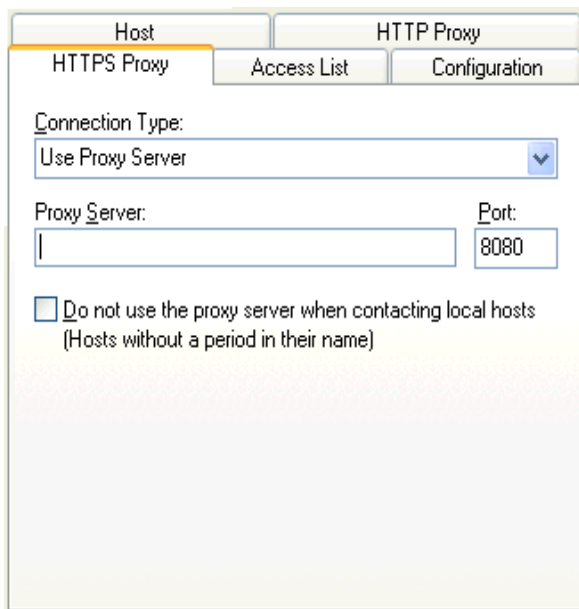
**Figure 10-1.** Configuring the HTTP Proxy tab

The following list describes the options and configurable parameters in the HTTP Proxy tab.

<b>Connection Type</b>	Indicates the type of connection for the host profile to use.  <b>Possible Values:</b> <Direct Connection> <Use Explorer Default> <Use Proxy Server>  <b>Default Value:</b> <Direct Connection>
<b>Proxy Server</b>	Indicates the location of the proxy server.  <b>Possible Values:</b> Any valid IP address, host name, or web address.  <b>Default Value:</b> <None>
<b>Port</b>	Indicates the network port for the proxy server.  <b>Possible Values:</b> Any valid port number.  <b>Default Value:</b> <8080>
<b>Do not use the proxy server when contacting local hosts</b>	Indicates whether the Telnet Client should use the proxy server when contacting hosts that reside on the same network.  <b>Possible Values:</b> <Enabled> <Disabled>  <b>Default Value:</b> <Disabled>

## HTTPS Proxy Tab

Use the HTTPS Proxy tab to configure secure proxy connections for WEB emulation.



**Figure 10-2.** *Configuring the HTTPS Proxy Tab*

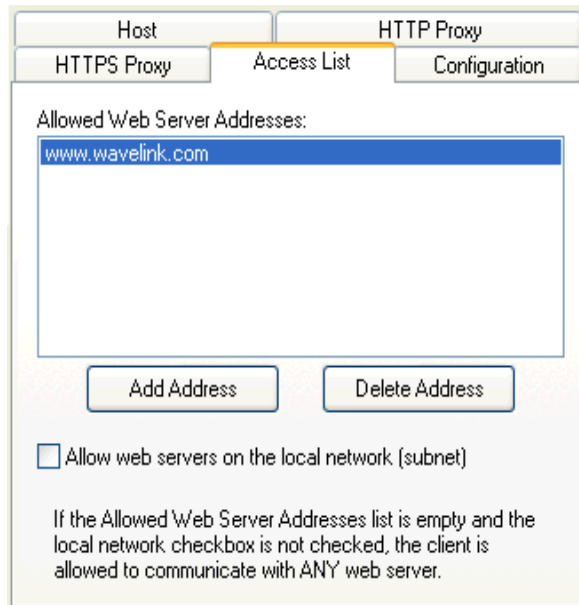
The following list describes the options and configurable parameters in the HTTPS Proxy tab.

- |                        |   |
|------------------------|---|
| <b>Connection Type</b> | Indicates the type of connection for the host profile to use.                         |
|                        | <b>Possible Values:</b> <Direct Connection> <Use Explorer Default> <Use Proxy Server> |
|                        | <b>Default Value:</b> <Direct Connection>   |
| <b>Proxy Server</b>    | Indicates the location of the proxy server  |
|                        | <b>Possible Values:</b> Any valid IP address, host name, or web address.              |
|                        | <b>Default Value:</b> <None>  |

<b>Port</b>	Indicates the network port for the proxy server. <b>Possible Values:</b> Any valid port number. <b>Default Value:</b> <8080>
<b>Do not use the proxy server when contacting local hosts</b>	Indicates whether the Telnet Client should use the proxy server when contacting hosts that reside on the same network. <b>Possible Values:</b> <Enabled> <Disabled> <b>Default Value:</b> <Disabled>

## Access List Tab

Use the Access List tab to configure which web addresses can be accessed by the Telnet Client Industrial Browser.



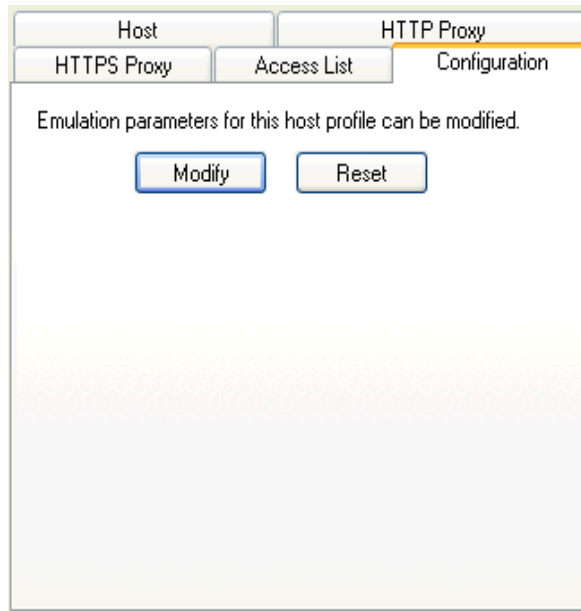
**Figure 10-3.** *Configuring the Access List Tab*

The following list describes the options and configurable parameters in the Access List tab.

<b>Allowed Web Server Addresses</b>	<p>Lists the web addresses that the Telnet Client is permitted to connect with.</p> <p><b>Possible Values:</b> Any valid IP address, host name, or web address.</p> <p><b>Default Value:</b> &lt;None&gt;</p>
<b>Allow web servers on the local network (subnet)</b>	<p>Indicates whether the Telnet Client can connect with any web server or only with servers on the local network.</p> <p><b>Possible Values:</b> &lt;Enabled&gt; &lt;Disabled&gt;</p> <p><b>Default Value:</b> &lt;Disabled&gt;</p>
<b>Add Address</b>	<p>Select this button to add a new IP or web address to the list of addresses that Telnet Client is permitted to connect with.</p>
<b>Delete Address</b>	<p>Select this button to delete any address in the list.</p>

## Configuration Tab

Use the Configuration tab to modify emulation parameters for the Host Profile.



**Figure 10-4.** *Configuration Tab*

Select `Modify` to access the Configuration Manager or `Reset` to restore default settings.

---

**NOTE** For more information about emulation parameters, refer to *Chapter 4: Emulation Parameters* on page 61.

---

## Using the Industrial Browser

This section provides information about using the Telnet Client Industrial Browser, including the following:

- Basic Navigation
- Specifying the Home Page

## Basic Navigation

The Telnet Client Industrial Browser interface provides basic commands for navigating web pages.

### To navigate within the Industrial Browser:

- 1 Connect to a WEB emulation session.
- 2 Tap and hold on the screen.

A menu appears.

- 3 From this menu, you can select from the following options:

<b>Back</b>	Returns the browser to the previous web page.
<b>Forward</b>	Returns to the screen displayed before <b>Back</b> was selected.
<b>Stop</b>	Stops the web page from loading.
<b>Refresh</b>	Reloads the current web page.
<b>Home</b>	Returns the browser to the specified home page.
<b>Text Size</b>	Displays a menu with the following text size options: <ul style="list-style-type: none"><li>• Largest</li><li>• Larger</li><li>• Medium</li><li>• Smaller</li><li>• Smallest</li></ul>

## Specifying the Home Page

The home page is the first page users will see when connecting to the Industrial Browser; it is also the page users will be returned to when they select **Home**. The home page will be the location you set up in the Host Profile for WEB emulation. This can either be an IP address or a specific web address. Refer to *Host Profile Settings* on page 197 for more information.



## Developing Web Pages for the Industrial Browser

This section provides information about the META tags and IDA commands supported by the Telnet Client Industrial Browser. You can use these tags to develop custom web pages that enable specific functionality in the Industrial Browser. The following information is included:

- META Tags
- IDA Commands

### META Tags

META tags are included at the top of a web page between the <HEAD> and </HEAD> tags. They are evaluated in the order they appear in the web page (from top to bottom). The Industrial Browser is designed to work only with tags it recognizes; it will ignore tags it does not recognize. If a META tag starts with the `iBrowse_` prefix, that prefix will be ignored. For example, `iBrowse_ScannerNavigate` is the same as `ScannerNavigate`.

Each META tag has the following format:

```
<meta http-equiv="action_name" content="action_type">
```

In the preceding format, the `action_type` can be a URL, an IDA action, or a JavaScript function. Some actions allow the action type to include replacement values; a `%s` or `%d` or `%ld` string can be used to indicate where each replacement item belongs.

---

**NOTE** These strings are interchangeable and can be used in any format that you prefer.

---

The following are META tags supported by the Telnet Client Industrial Browser:

- `BatteryNavigate`
- `OnAllKeys`, `OnKey...`, `OnKey0x...`
- `OnStartup`, `IDA`
- `PowerOn`

- Printing
- Scanner
- ScannerNavigate, ScannerProcessed
- SignalNavigate
- SpeechFromText
- SpeechSetting
- TextFromSpeech
- Symbolologies

### **BatteryNavigate**

The `BatteryNavigate` META tag is used to handle changes in the battery strength or the AC line status. The action occurs when the battery strength changes or when the device is plugged in or unplugged.

The four arguments (from left to right) are: the AC line status, the strength of the main battery from zero to 100, the strength of the backup battery from zero to 100, and the main battery chemistry. A battery strength of 255 means "unknown."

The following are the AC line status values:

```
#define AC_LINE_OFFLINE           00
#define AC_LINE_ONLINE           01
#define AC_LINE_BACKUP_POWER     02
#define AC_LINE_UNKNOWN          255
```

The following are the battery chemistry values:

```
BATTERY_CHEMISTRY_ALKALINE      01
BATTERY_CHEMISTRY_NICD          02
BATTERY_CHEMISTRY_NIMH          03
BATTERY_CHEMISTRY_LION          04
BATTERY_CHEMISTRY_LIPOLY        05
BATTERY_CHEMISTRY_ZINCAIR       06
BATTERY_CHEMISTRY_UNKNOWN       255
```

### **OnAllKeys, OnKey..., OnKey0x...**

The `OnKey...` and `OnKey0x...` META tags describe an action that will occur if a particular key is pressed. The key values that are evaluated are the same key values used by Keyboard Creator.

The `OnKey0x` format requires a hexadecimal number, while the `OnKey` format will require a decimal format. The key value is also case sensitive.

For example:

`OnKey50` and `OnKey0x32` will both respond to the 2 key.

`OnKey65` and `OnKey97` would be used to respond to both the upper and lowercase A.

The `OnAllKeys` tag will perform the prescribed action each time a key is pressed. The action type can include one argument, which is the string representing the decimal value of the key.

---

**NOTE** Due to browser limitations, some keys (such as `Tab`) may not always be handled by this tag.

---

### **OnStartup, IDA**

The `OnStartup` and `IDA` META tags allow you to specify actions that will be taken when the web page is first loaded. The action type must be one of the action types described in *IDA Commands* on page 175.

### **PowerOn**

The `PowerOn` META tag is used when the device turns on.

### **Printing**

You can send data to the printer by including the data in the META tags. Use the `Print_Continue` and `Print_Finish` action names to specify the print data. The print data is in the action type of these META tags. The print data in each META tag should all be on the same line and should not be more than 1024 characters in length; however the total print data can be larger than 1024 characters. In addition to standard characters, you can use the following:

- `\r` to specify a return character
- `\n` to specify a newline character

- `\t` to specify a tab character
- `\\` to specify a backslash character
- `\##` or `\x##` to specify any other character, where `##` is replaced with a two-digit hexadecimal number

`Print_Continue` should be used for all but the last section of print data, and `Print_Finish` should be used for the last section of print data.

---

**NOTE** If desired, the action names `Print_Done`, `Print_Final`, `PLSeriesLabel_Print` and `ZebraLabel_Print` can be used instead of `Print_Finish`.

---

The META tag `Print_Callback` can be used to specify the action that will occur after the printing is completed. The argument will be 0 if the printing was successful, or a non-zero number if the printing failed.

---

**NOTE** If desired, the action names `Print_Complete`, `ZebraLabel_Complete` and `PLSeriesLabel_Complete` can be used instead of `Print_Callback`.

---

The META tag `Print_Setup_TP` can be used to specify the IP Address and port of the printer if using TCP printing. If this tag is used, it must be specified before the `Print_Finish` tag. The format is `address:port`.

For example:

```
<meta http-equiv="Print_Setup_TP"
content="192.168.1.59:7429">
```

```
<meta http-equiv="Print_Continue"
content="\22First Line\22\r\n">
```

```
<meta http-equiv="Print_Continue"
content="\22Middle\22\r\n">
```

```
<meta http-equiv="Print_Finish"
content="\22Last Line\22\r\n">
```

```
<meta http-equiv="Print_Callback"  
content="printresult.htm&status=%s"
```

### Scanner

If the action name is `Scanner` and the action type is `Enable` or `Resume`, the scanner will be enabled when the page is first loaded. If the action type is `Disable` or `Suspend`, the scanner will be disabled when the page is first loaded.

There are four additional scanner action types supported by Telnet Client Industrial Browser:

- `AutoTab`
- `AutoEnter`
- `AutoEnterAndTab`
- `NoAuto`

The `AutoTab`, `AutoEnter`, and `AutoEnterAndTab` action types will enable the scanner and will cause the scan data to be followed by an enter or tab key (or both). The `NoAuto` action type will enable the scanner and will clear the scanner key value (if a value is specified by the emulation parameters).

Once enabled or disabled, the scanner will stay in that state until some other action (such as a META tag or IDA action) changes the state or until the user changes sessions.

You can also use `WEB Default Scanner Auto Keys` and `WEB Default Scanner State` emulation parameters to configure the default scanner action on web pages with no applicable META tags. For more information on emulation parameters, see *Manually Configuring Emulation Parameters* on page 201.

### ScannerNavigate, ScannerProcessed

The `ScannerNavigate` META tag is used to handle raw scan data. The `ScannerProcessed` tag is similar, but gives the scan data after it has been modified by the scan handlers, etc. in the Emulation Parameters.

If the action type has zero to three arguments, then the arguments are (from left to right): the barcode data, the symbology type, and the time stamp.

If the action type has four or five arguments, then the arguments are (from left to right): the barcode data, source scanner name, symbology type, time stamp, and barcode length.

---

**NOTE** Refer to the Symbologies section for supported symbology types.

---

### **SignalNavigate**

The `SignalNavigate` META tag is used to handle changes in the signal strength of the wireless network connection. The action occurs when the signal strength changes or when the device disconnects from the wireless network.

The three arguments (from left to right) are: signal strength, connected ESSID, and device MAC address. The signal strength is zero to 100. Strength `-1` means "unknown." Strength `-2` means "disconnected from the wireless network." ESSID and MAC addresses may be "`<unknown>`." (Available on Windows-CE devices only.)

### **SpeechFromText**

The `SpeechFromText` META tag plays the string specified by the "content" flag.

For example:

```
<meta http-equiv="SpeechFromText" content="I will speak  
this sentence.">
```

### **SpeechSetting**

The `SpeechSetting` META tag changes one or more speech values.

For example:

The following META tag will change the Text-to-Speech settings for language and voice:

```
<meta http-equiv="SpeechSetting"  
content="tts_language=American English, tts_voice=Tom">
```

### **TextFromSpeech**

The `TextFromSpeech` META tag will play the string specified by the "content" flag. This META tag function is identical to the `SpeechFromText` META tag.

## Symbologies

It is possible to enable and disable different symbologies by using the symbology as the action name, and `Enabled` or `Disabled` as the action type. The symbologies supported by Telnet Client Industrial Browser are as follows:

AUSTRALIA_POSTAL	CUECODE	PLANET
AZTEC	D2OF1ATA	PLESSY
AZTECMESA	D2OF5	POSICODE
BOOKLAND	DATAMATRIX	POSTNET
BRITISH_POSTAL	DUTCH_POSTAL	QRCODE
CANADA_POSTAL	EAN8	RSS14
CHINA_POSTAL	EAN13	RSSEXPANDED
CODABAR	I2OF5	RSSLIMITED
CODABLOCK	JAPAN_POSTAL	SIGNATURE
CODE11	KOREA_POSTAL	TELEPEN
CODE16K	MACROPDF	TLC39
CODE32	MACROMICROPDF	TRIOPTIC39
CODE39	MAXICODE	UCC128
CODE49	MATRIX2OF5	UPCA
CODE93	MICROPDF	UPCE
CODE128	MSI	UPCE0
COMPOSITE	OCR	UPCE1
COUPONCODE	PDF417	WEBCODE

In addition to the preceding symbologies, the value `ALL_DECODERS` can be used to enable or disable all the symbologies.

For example:

To enable only UPCA, use the META tags in this order

```
<meta http-equiv="ALL_DECODERS" content="Disabled">
```

```
<meta http-equiv="UPCA" content="Enabled">
```

The prefix `Scanner_` can also be used with all symbologies.

## Element-Specific Actions

The following META tag options are also supported for individual elements:

- `OnAllKeys`, `OnKey...`, `OnKey0x...`

- Scanner
- Symbologies

The options can be specified in the tag that creates the element on the web page. If the element is selected (active), then the option will be applied. When the tag is not selected (inactive), then the settings will revert back to those specified by the META tags for the web page.

Unlike the META tags, where "http-equiv" is used to specify the action name and "content" is used to specify the action type, a simple action\_name="action type" format is used.

For example:

The following tag will cause the Scanner to be enabled when the tag is selected on the web page.

```
<input name="item1" id="item1" type="text"
Scanner="Enable">
```

The following tag will enable the scanner only while the tag is selected. The scanner will be disabled otherwise.

```
<meta http-equiv="Scanner" content="Disable">
```

---

**NOTE** You can use the META tag `OnStartup` with an action of `IDA_SCAN_ENABLE` or `IDA_SCAN_DISABLE` to change the scanner state only when the page is first loaded.

---

To use element-specific Symbologies, you can either use the Symbology name or prefix the Symbology name with the string "Scanner\_".

For example:

The following tag will enable the scanner, AutoTab after an item is scanned, and turn off all Symbologies except Code128.

```
<textarea name="item2" Scanner=AutoTab
Scanner_All_Decoders=Disable Scanner_Code128=Enable>
```



---

**NOTE** The Code128 enable item must come after the All\_Decoders item or it will be disabled when the All\_Decoders item is processed.

---

## IDA Commands

IDA commands are special values used to invoke a device action, program action, or emulator action within the Telnet Client Industrial Browser. These values can be specified in many of the special META tags described above, as URLs for the user to click on, or called inside JavaScript functions.

For example:

```
<a href="ida:IDA_SESSION_DISCONNECT">
Close the session</a>
```

-Or-

```
<script language=javascript>
function OnError( )
{
    // Disconnect the Session
    location.href = "ida:IDA_SESSION_DISCONNECT" ;

    // Alternate Method
    document.location = "ida:IDA_SESSION_DISCONNECT" ;

    // Another Alternate Method
    window.navigate ( "ida:IDA_SESSION_DISCONNECT" ) ;
}
</script>
```

---

**NOTE** It is recommended that each IDA command be preceded by the `ida` prefix; however, the command will generally work without the prefix.

---

The following are IDA commands supported by the Telnet Client Industrial Browser:

- IDA\_COLDBOOT
- IDA\_COLDBOOT\_PROMPT

- IDA\_KEYBOARD\_WEB, IDA\_KEYBOARD\_SHOW, or IDA\_KEYBOARD\_UP
- IDA\_KEYBOARD\_NUM or IDA\_KEYBOARD\_NUMERIC
- IDA\_KEYBOARD\_NONE, IDA\_KEYBOARD\_HIDE, or IDA\_KEYBOARD\_DOWN
- IDA\_PROGRAM\_EXIT
- IDA\_PROGRAM\_EXIT\_PROMPT
- IDA\_REPRINT
- IDA\_SCAN\_DISABLE or IDA\_SCAN\_SUSPEND
- IDA\_SCAN\_ENABLE or IDA\_SCAN\_RESUME
- IDA\_SCAN\_FORWARD
- IDA\_SESSION\_S1, IDA\_SESSION\_S2, IDA\_SESSION\_S3, IDA\_SESSION\_S4
- IDA\_SESSION\_DISCONNECT
- IDA\_SESSION\_DISCONNECT\_PROMPT
- IDA\_SESSION\_NEXT
- IDA\_SESSION\_PREVIOUS
- IDA\_SIP\_SHOW or IDA\_SIP\_UP
- IDA\_SIP\_HIDE or IDA\_SIP\_DOWN
- IDA\_SIP\_TOGGLE or IDA\_SIP\_TOGGLEHIDE
- IDA\_SUSPEND or IDA\_SUSPEND\_DEVICE
- IDA\_SUSPEND\_PROMPT
- IDA\_URL\_BACK or IDA\_BACK
- IDA\_URL\_BACK\_DISABLE or IDA\_BACK\_DISABLE

- IDA\_URL\_BACK\_ENABLE or IDA\_BACK\_ENABLE
- IDA\_URL\_FORWARD or IDA\_FORWARD
- IDA\_URL\_FORWARD\_DISABLE or IDA\_FORWARD\_DISABLE
- IDA\_URL\_FORWARD\_ENABLE or IDA\_FORWARD\_ENABLE
- IDA\_URL\_HOME or IDA\_HOME
- IDA\_URL\_HOME\_DISABLE or IDA\_HOME\_DISABLE
- IDA\_URL\_HOME\_ENABLE or IDA\_HOME\_ENABLE
- IDA\_URL\_REFRESH or IDA\_REFRESH
- IDA\_URL\_STOP or IDA\_STOP
- IDA\_WARMBOOT
- IDA\_WARMBOOT\_PROMPT
- IDA\_ZOOM\_DISABLE or IDA\_FONT\_DISABLE
- IDA\_ZOOM\_ENABLE or IDA\_FONT\_ENABLE
- IDA\_ZOOM\_LARGER or IDA\_FONT\_LARGER
- IDA\_ZOOM\_LARGEST or IDA\_FONT\_LARGEST
- IDA\_ZOOM\_MEDIUM or IDA\_FONT\_MEDIUM
- IDA\_ZOOM\_MINUS or IDA\_FONT\_MINUS
- IDA\_ZOOM\_PLUS or IDA\_FONT\_PLUS
- IDA\_ZOOM\_SMALLER or IDA\_FONT\_SMALLER
- IDA\_ZOOM\_SMALLEST or IDA\_FONT\_SMALLEST

### **IDA\_COLDBOOT**

This command causes the device to perform a cold boot.

**IDA\_COLDBOOT\_PROMPT**

This command gives the user the option to perform a cold boot or cancel the action.

**IDA\_KEYBOARD\_WEB, IDA\_KEYBOARD\_SHOW, or IDA\_KEYBOARD\_UP**

These commands cause the emulation on-screen keyboard to be displayed.

**IDA\_KEYBOARD\_NUM or IDA\_KEYBOARD\_NUMERIC**

These commands cause the numeric on-screen keyboard to be displayed.

**IDA\_KEYBOARD\_NONE, IDA\_KEYBOARD\_HIDE, or IDA\_KEYBOARD\_DOWN**

These commands cause the emulation and numeric on-screen keyboards to be hidden.

**IDA\_PROGRAM\_EXIT**

This command causes the device to exit the current program.

**IDA\_PROGRAM\_EXIT\_PROMPT**

This command gives the user the option to exit the program or cancel the action.

**IDA\_REPRINT**

This command causes the last data supplied to the printer to be sent again. The print data will remain available until something else is printed or until the session is disconnected.

**IDA\_SESSION\_S1, IDA\_SESSION\_S2, IDA\_SESSION\_S3, IDA\_SESSION\_S4**

These commands cause the device to switch to the specified session.

**IDA\_SCAN\_DISABLE or IDA\_SCAN\_SUSPEND**

These commands disable the bar code scanner. When the bar code scanner is disabled, pressing the mobile device trigger will have no effect.

**IDA\_SCAN\_ENABLE or IDA\_SCAN\_RESUME**

These commands enable the bar code scanner. The bar code scanner will not actually scan for bar codes unless the mobile device trigger is pulled.

---

**NOTE** You can use the META tag `OnStartup` with an action of `IDA_SCAN_ENABLE` or `IDA_SCAN_DISABLE` to change the scanner state only when the page is first loaded.

---

### **IDA\_SCAN\_FORWARD**

This command disables the barcode scanner and processes a trigger press as a key press. This command only functions on scanners that support trigger-press forwarding; on all other scanners, the command performs the same action as `IDA_SCAN_DISABLE`.

### **IDA\_SESSION\_DISCONNECT**

This command disconnects the session and closes the Industrial Browser.

### **IDA\_SESSION\_DISCONNECT\_PROMPT**

This command gives the user the option to disconnect the session and close the Industrial Browser, or cancel the action.

### **IDA\_SESSION\_NEXT**

This command causes the device to switch to the next-higher numbered session (I.e. From session two to session three). If the device is currently on the last session, the device will switch to session one.

### **IDA\_SESSION\_PREVIOUS**

This command causes the device to switch to the next-lower numbered session (I.e. From session three to session two). If the device is currently on session one, the device will switch to the last session.

### **IDA\_SIP\_SHOW or IDA\_SIP\_UP**

These commands cause the SIP on-screen keyboard to become visible.

### **IDA\_SIP\_HIDE or IDA\_SIP\_DOWN**

These commands cause the SIP on-screen keyboard to become hidden.

### **IDA\_SIP\_TOGGLE or IDA\_SIP\_TOGGLEHIDE**

These commands will cause the SIP on-screen keyboard to become visible if it is hidden, or hidden if it is visible.

### **IDA\_SUSPEND or IDA\_SUSPEND\_DEVICE**

These commands cause the device to suspend itself.

---

**NOTE** For CE devices, this is similar to pressing the power button.

---

### **IDA\_SUSPEND\_PROMPT**

This command gives the user the option to suspend the device or cancel the action.

### **IDA\_URL\_BACK or IDA\_BACK**

These commands cause the Industrial Browser to display the screen previous to the current screen. If there are no previous screens, no action will be taken.

### **IDA\_URL\_BACK\_DISABLE or IDA\_BACK\_DISABLE**

These commands disable the `Back` menu option so it cannot be selected by the user.

---

**NOTE** The `IDA_URL_BACK` or `IDA_BACK` commands are not affected and will still work.

---

### **IDA\_URL\_BACK\_ENABLE or IDA\_BACK\_ENABLE**

These commands enable the `Back` menu option so it can be selected by the user. The menu option could still be disabled if there is no page to go back to.

### **IDA\_URL\_FORWARD or IDA\_FORWARD**

These commands cause the Industrial Browser to display the screen that was being displayed before the last `Back` command. If there was no previous screen, no action will be taken.

### **IDA\_URL\_FORWARD\_DISABLE or IDA\_FORWARD\_DISABLE**

These commands disable the `Forward` menu option so it cannot be selected by the user.

---

**NOTE** The `IDA_URL_FORWARD` or `IDA_FORWARD` commands are not affected and will still work.

---

### **IDA\_URL\_FORWARD\_ENABLE or IDA\_FORWARD\_ENABLE**

These commands enable the `Forward` menu option so it can be selected by the user.

---

**NOTE** The menu option could still be disabled if there is no page to return to.

---

### **IDA\_URL\_HOME or IDA\_HOME**

These commands cause the Industrial Browser to proceed to the location specified by the current Host Profile. It is completely independent from the Home location for any other web browsers on the device.

### **IDA\_URL\_HOME\_DISABLE or IDA\_HOME\_DISABLE**

These commands disable the Home menu option so it cannot be selected by the user.

---

**NOTE** The IDA\_URL\_HOME or IDA\_HOME commands are not affected and will still work.

---

### **IDA\_URL\_HOME\_ENABLE or IDA\_HOME\_ENABLE**

These commands enable the Home menu option so it can be selected by the user.

### **IDA\_URL\_REFRESH or IDA\_REFRESH**

These commands cause the web page to be reloaded. The server will be queried to verify that the page contents are up-to-date.

### **IDA\_URL\_STOP or IDA\_STOP**

These commands cause the web page to stop loading. If the web page is already fully loaded, this action has no effect.

### **IDA\_WARMBOOT**

This command causes the device to perform a warm boot.

### **IDA\_WARMBOOT\_PROMPT**

This command gives the user the option to perform a warm boot or cancel the action.

### **IDA\_ZOOM\_DISABLE or IDA\_FONT\_DISABLE**

These commands disable the Text Size menu to be disabled so it cannot be selected by the user.

---

**NOTE** The IDA options to set the zoom level (text size) are not affected and will still work.

---

**IDA\_ZOOM\_ENABLE or IDA\_FONT\_ENABLE**

These commands enable the **Text Size** menu so it can be selected by the user.

**IDA\_ZOOM\_LARGER or IDA\_FONT\_LARGER**

These commands cause the Industrial Browser to display the text using a large text size.

---

**NOTE** This is a global setting. Other Telnet sessions, Internet Explorer, and Pocket Internet Explorer will default to using this text size as well.

---

**IDA\_ZOOM\_LARGEST or IDA\_FONT\_LARGEST**

These commands cause the Industrial Browser to display the text using the largest text size supported by the browser.

---

**NOTE** This is a global setting. Other Telnet sessions, Internet Explorer, and Pocket Internet Explorer will default to using this text size as well.

---

**IDA\_ZOOM\_MEDIUM or IDA\_FONT\_MEDIUM**

These commands cause the Industrial Browser to display the text using a medium text size.

---

**NOTE** This is a global setting. Other Telnet sessions, Internet Explorer, and Pocket Internet Explorer will default to using this text size as well.

---

**IDA\_ZOOM\_MINUS or IDA\_FONT\_MINUS**

These commands cause the Industrial Browser to display the text using the next-smaller text size than the current text size.

---

**NOTE** This is a global setting. Other Telnet sessions, Internet Explorer, and Pocket Internet Explorer will default to using this text size as well.

---



---

**IDA\_ZOOM\_PLUS or IDA\_FONT\_PLUS**

These commands cause the Industrial Browser to display the text using the next-larger text size than the current text size.

---

**NOTE** This is a global setting. Other Telnet sessions, Internet Explorer, and Pocket Internet Explorer will default to using this text size as well.

---

**IDA\_ZOOM\_SMALLER or IDA\_FONT\_SMALLER**

These commands cause the Industrial Browser to display the text using a small text size.

---

**NOTE** This is a global setting. Other Telnet sessions, Internet Explorer, and Pocket Internet Explorer will default to using this text size as well.

---

**IDA\_ZOOM\_SMALLEST or IDA\_FONT\_SMALLEST**

These commands cause the Industrial Browser to display the text using the smallest text size supported by the browser.

---

**NOTE** This is a global setting. Other Telnet sessions, Internet Explorer, and Pocket Internet Explorer will default to using this text size as well.

---



## Chapter 11: Avalanche Integration

This section provides the following information:

- Overview of Avalanche Integration
- Using Session Monitor
- Using Real-Time Statistics

### Overview of Avalanche Integration

A number of additional features are available for the Telnet Client when you choose to install the Telnet Client via the Avalanche framework.

Avalanche-installed Telnet Clients offer the following Avalanche-integrated features:

- **Session Monitor.** Allows you to monitor and to take control of the Telnet Client remotely from the Avalanche Management Console.
- **Real-Time Statistics.** Allows you to view real-time statistics, including session length and number of scans, from the *Avalanche Client Controls* dialog box in the Avalanche Management Console.

To take advantage of the Avalanche features of the Telnet Client, your Avalanche environment must meet the following requirements:

- Avalanche Manager 3.5 (or greater version) for Session Monitor
- Avalanche Manager 3.4 (or greater version) for Real-Time Statistics
- Avalanche Enabler 3.x (or greater version)
- A valid Avalanche license for the mobile device running the Telnet Client
- A valid platform or maintenance license for the Telnet Client
- Telnet Client 5.x (or greater version)

## Using Session Monitor

The Session Monitor utility allows you to view the Telnet Client on a mobile device from the Avalanche Management Console. Session Monitor includes an override feature that allows you to take control of the Telnet Client on the mobile device. Session Monitor also includes a logging feature that allows you to create a trace for Telnet sessions.

This sections provides the following information:

- Enabling Session Monitor
- Configuring Session Monitor
- Launching Session Monitor
- Session Override
- Tracing Sessions

---

**NOTE** Session Monitor requires Avalanche Manager 3.5 (or greater version) and a valid Avalanche license.

---

### Enabling Session Monitor

The following tasks are required to enable Session Monitor.

- 1 Install the Telnet Client package in Avalanche Manager.
- 2 Configure the Telnet Client to use Session Monitor.
- 3 Perform an Avalanche update to deploy the Telnet Client to the mobile device.
- 4 Launch the Telnet Client on the mobile device.
- 5 Launch Session Monitor from Avalanche Manager.

### Configuring Session Monitor

Configure the following Session Monitor parameters in the Telnet Emulation Parameters:

- **Session Monitor Address.** These are the IP addresses of computers that the Telnet Client allows to do session monitoring. If no addresses are specified, the Telnet allows session monitoring from any computer.
- **Session Monitor Override Timeout.** This is the maximum number of minutes that Session Monitor is allowed to override the session. After the time expires, the override setting is disabled and control returns to the client device. The default time-out for override mode is set to 0 (never). This means the override mode will never time-out and the client regains control only if override mode is disabled manually.
- **Session Monitor Password.** This is the password required for Session Monitor connections. The password is loaded in the Emulation Parameters file and is never entered by the user. It has a 63 character limit. If no password is entered, the Telnet Client will not accept Session Monitor connections.
- **Session Monitor Port.** This is the port that the Telnet Client listens to for Session Monitor connections.

#### **To configure Session Monitor**

- 1 Locate the Telnet Client software package in the Tree View of the Avalanche Manager.
- 2 Right-click the software package.
- 3 Select `Configure Package > Emulation Parameters`.  
Configuration Manager launches.
- 4 Expand the Emulation folder.
- 5 Expand the Session Monitor folder.
- 6 Double-click the Session Monitor menu items to change the parameters.

---

**NOTE** The Session Monitor Password is the only required configuration. The other parameters are optional configurations.

---

- 7 Once you have configured the Session Monitor parameters, click the Save button.

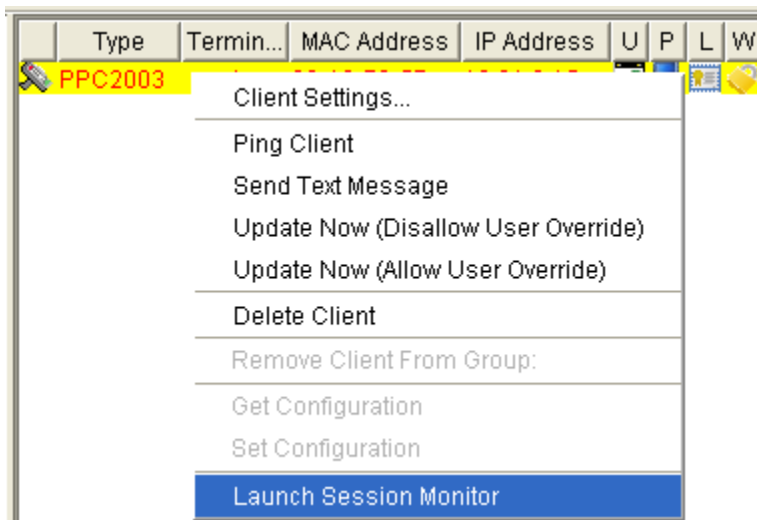
- 8 Close the configuration utility.
- 9 Perform an Avalanche update to download the new configuration to the mobile device.

## Launching Session Monitor

You can launch Session Monitor from the Avalanche Management Console.

### To launch Session Monitor

- 1 From the Device View of Management Console, right-click the device you want to monitor.
- 2 Select the `Launch Session Monitor` option.



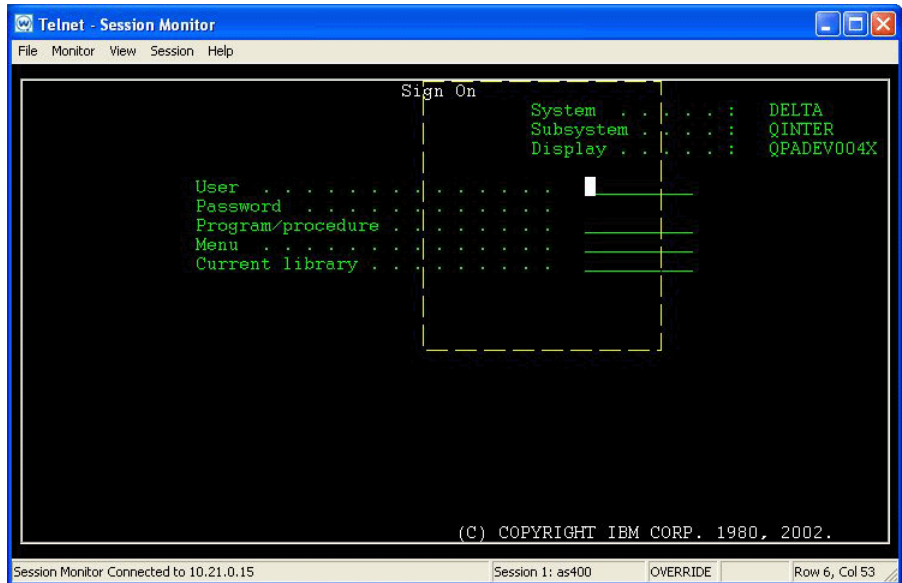
**Figure 11-1.** *Launching Session Monitor*

---

**NOTE** The client device and the Avalanche Manager need to be communicating over the network.

---

The Telnet Session Monitor screen opens and connects to the session. The yellow-lined box represents what the device user can see.



**Figure 11-2.** Connecting to Session Monitor

---

**NOTE** If both the mobile device and the Avalanche PC have SSL support installed, the Session Monitor network information will be encrypted.

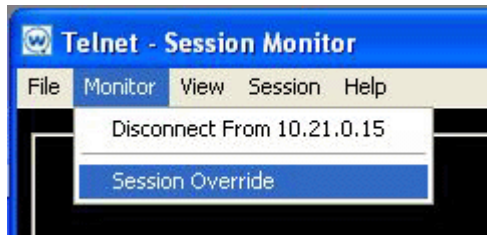
---

## Session Override

Use the session override option of Session Monitor to take control of the Telnet Client. When you enable session override, the mobile device user will not be able to interact with the Telnet Client.

### To enable override mode

- 1 In Session Monitor, access the Monitor menu.
- 2 Select the Session Override option.



**Figure 11-3.** *Enabling Session Override*

The session remains in override mode until the override timeout minutes expire or until you manually disable the session override option.

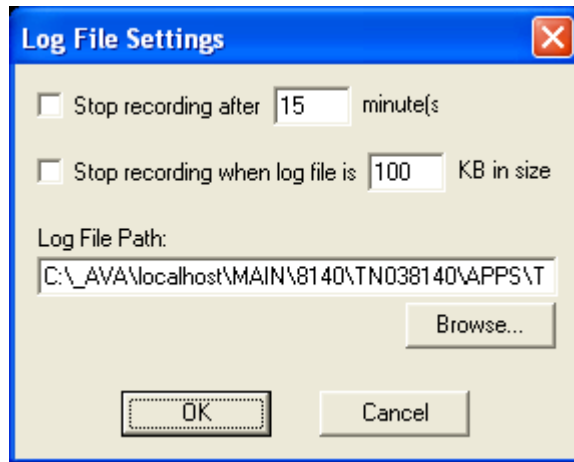
## Tracing Sessions

Use the *Log File Settings* dialog box to configure the Session Monitor log file to trace Session Monitor sessions.

### To trace a session

- 1 In Session Monitor, access the *File* menu.
- 2 Select the *Log to File* option.
- 3 Configure the log file settings.
- 4 In the *Log File Path* text box, enter the path to the directory where you want to save the log file.
- 5 Click *OK*.





**Figure 11-4.** *Configuring Log File Settings*

---

**NOTE** The log file is saved as `sessionlog.txt` in the directory specified in Log File Path text box. If `sessionlog.txt` already exists, the log file will attempt to save as `sessionlog2.txt`, `sessionlog3.txt`, etc. until it finds a non-existing file name in the specified log file path.

---

## Using Real-Time Statistics

The Telnet Client periodically transmits emulation-specific information to Avalanche Manager. Avalanche Manager displays the information it receives in the Properties tab of the *Avalanche Client Controls* dialog box for the mobile device.

The Avalanche Manager displays Telnet session information including:

- **Telnet-Specific Information.** This includes information on the current Telnet Client version, the mobile device battery power, and SSL support and use.
- **Session-Specific Information.** This includes information on barcode, MSR and RFID scanning, session connect time, and running time of the current session.

By default, the Telnet Client transmits emulation-specific information to Avalanche Manager every five minutes (300 seconds). You can modify this `RealTimeStatsInterval` property in the Properties tab of the *Avalanche Client Controls* dialog box.

This document provides the following information:

- Viewing real-time statistics
- Modifying real-time statistics

---

**NOTE** Real-Time Statistics requires Avalanche Manager 3.4 (or greater version) and a valid Avalanche license for the mobile device.

---

## Viewing Real-Time Statistics

You can view the real-time statistics from the Properties tab of the *Avalanche Client Controls* dialog box.

### To view the statistics:

- 1 From the Device View of Management Console, right-click the device you want to monitor.
- 2 Select `Client Settings`.

The *Avalanche Client Controls* dialog box opens.

- 3 Click the Properties tab.

The Properties tab contains a number of entries specific to the Telnet Client.

Property	Value	Changeable	Change Pending
RogueScan.APDelay	3600	Yes	
RogueScan.AgeOut	24	Yes	
RogueScan.DeviceIdle	10	Yes	
RogueScan.DeviceTime	100	Yes	
RogueScan.Filter	1	Yes	
RogueScan.Supported	0		
Series	C		
SetClock	1	Yes	
TerminalID	1	On Control page	
Telnet.Version	5.00-01	Yes	
Telnet.SSL Supported	Yes	Yes	
Telnet.Battery Power	External Power	Yes	
Telnet.Average Time Total	600	Yes	
Telnet.Average Time Display	60	Yes	
Telnet.Time Running	1.8 Minutes	Yes	
Telnet.Session 1.Connect Time	10.0 Minutes	Yes	
Telnet.Session 1.SSL In Use	No	Yes	
Telnet.Session 1.Barcode Scans	0.0 Scans per Minute	Yes	
Telnet.Session 1.MSR Scans	0.0 Scans per Minute	Yes	
Telnet.Session 1.Transactions	0.4 per Minute	Yes	

**Figure 11-5.** Viewing Real-Time Statistics in Avalanche Manager

The following list describes the Telnet Client real-time statistics that are displayed in the Properties tab.

**RealTimeStatsInterval** Indicates how often the Telnet Client sends real-time statistics information to Avalanche Manager. The interval is measured in seconds.

Default: 300 seconds

Note: It is recommended to change the time to five (5) seconds when you are monitoring a device.

**Telnet Version** Displays the current version of the Telnet Client.

**Telnet SSL Supported** Indicates whether SSL is supported.

**Telnet Battery Power** Indicates the remaining battery power of the mobile device.

---

<b>Telnet Average Time Total</b>	Indicates the length of time the session statistics are tracked.  <b>Default:</b> 600 seconds
<b>Telnet Average Time Display</b>	Indicates the interval time for barcode, MSR, and RFID scans and transactions. The default setting (60 seconds) means that scans display as a number of scans per minute. If you change this to property to 120 seconds, the scans display as number of scans per two minutes.  <b>Default:</b> 60 seconds
<b>Telnet Time Running</b>	Displays the current running time for the Telnet Client.
<b>Telnet Session &lt;n&gt; Connect Time</b>	Displays the amount of time the Telnet session has been running, where <n> indicates the Telnet session (1 - 4).
<b>Telnet Session &lt;n&gt; SSL in Use</b>	Indicates whether the Telnet session is using SSL, where <n> indicates the Telnet session (1-4).
<b>Telnet Session &lt;n&gt; Barcode Scans</b>	Displays the number of barcode scans per <x> seconds for the Telnet Session, where <n> indicates the Telnet session (1-4) and <x> indicates the time set in the Telnet Average Time Display property.
<b>Telnet Session &lt;n&gt; MSR Scans</b>	Displays the number of MSR scans per <x> seconds for the Telnet Session, where <n> indicates the Telnet session (1-4) and <x> indicates the time set in the Telnet Average Time Display property.  MSR scan information displays only if the mobile device supports MSR scanning.

**Telnet Session <n> Transaction** Displays the number of transactions per <x> seconds for the Telnet Session, where <n> indicates the Telnet session (1–4) and <x> indicates the time set in the Telnet Average Time Display property.

**Telnet Session <n> RFID** Displays the number of RFID scans per <x> seconds for the Telnet Session, where <n> indicates the Telnet session (1–4) and <x> indicates the time set in the Telnet Average Time Display property.

RFID scan information displays only if the mobile device supports RFID scanning.

## Modifying Real-Time Statistics

While many of the Telnet session parameters indicate they are changeable, you should only modify `RealTimeStatsInterval`, `Telnet Average Time Total`, and `Telnet Average Time Display`.

### To modify a statistic:

- 1 From the Device View of Management Console, right-click the device you want to monitor.
- 2 Select `Client Settings`.  
The *Avalanche Client Controls* dialog box opens.
- 3 Click the Properties tab.
- 4 Click the Value column of the statistic you want to change.
- 5 Type the new Value.
- 6 Click the `Apply Changes` button.
- 7 Update the device to download the new property values to the device.

---

**NOTE** If the Telnet Client is currently running, modified real-time statistics will not display until the next real-time statistics transmit to Avalanche Manager. For example, if you modify the `RealTimeStatsInterval` property

from 300 seconds to five (5) seconds, it may take the remaining seconds of the previous 300-second setting before the statistics begin to update every five seconds.

---

## Chapter 12: Manually Configuring the Telnet Client

This section provides the following information:

You can configure certain Telnet Client parameters manually (that is, at the mobile device), including:

- Manually Configuring Host Profiles
- Manually Configuring Emulation Parameters

### Manually Configuring Host Profiles

You can manually perform the following tasks with the Telnet Client interface:

- Creating a New Host Profile
- Modifying an Existing Host Profile
- Deleting an Existing Host Profile

---

**NOTE** When you download a new Telnet Client configuration to the mobile device using Microsoft ActiveSync or Avalanche Manager, any manual changes that you have made will be overwritten.

---

---

**NOTE** For information about host profiles, see *Chapter 3: Host Profiles* on page 29.

---

### Accessing Host Profiles

To add, modify, or delete host profile, you must access the *Host Profiles* dialog box.

**To access the host profiles dialog box:**

- 1 On the mobile device, launch the Telnet Client.
- 2 In the Telnet Client, access the **Options** menu.

- 3 From the **Options** menu, select `Configure > Host Profiles`.

The *Input Password* dialog box appears.

- 4 In the **Input Host Config Password** text box, type the RF Config Password.

---

**NOTE** The default RF Config Password is “system”. For information about modifying the RF Config Password, see *Configuring Passwords* on page 235. If no RF Config Password is configured, the Telnet Client will not prompt you for a password.

---

- 5 Press the `Enter` key.

The *Edit Host Profile* dialog box appears.

- 6 Use the *Edit Host Profile* dialog box to add, modify, or delete host profiles.

## Creating a New Host Profile

You can use the *Edit Host Profile* dialog box to create a new host profile for the Telnet Client.

### To create a new host profile:

- 1 On the mobile device, launch the Telnet Client.
- 2 Use the Telnet Client **Options** menu to access the *Edit Host Profiles* dialog box.
- 3 In the *Edit Host Profile* dialog box, click `Add`.  
  
A new *Edit Host Profile* dialog box appears.
- 4 Use the *Edit Host Profile* dialog box to configure the basic parameters of the host profile (alias, IP address, TCP port number, and emulation type).
- 5 Select `More` to access and configure other configuration parameters that are specific to the emulation type that you have selected.

---

**NOTE** For more information about other configurable parameters for a host profile, see *Host Profile Settings* on page 201.

---



- 6 After you have finished configuring the host profile, select `Save` in the *Edit Host Profile* dialog box.

The *Edit Host Profiles* dialog box appears, and you are returned to the first *Edit Host Profile* dialog box, which now displays the new host profile.

- 7 Select `Done`.

The *Edit Host Profile* dialog box closes and you return to the primary Telnet Client interface.

---

**NOTE** To exit either of the *Edit Host Profile* dialog box without saving the changes that you have made, press `Esc`.

---

## Modifying an Existing Host Profile

You can use the *Edit Host Profile* dialog box to modify the parameters of an existing host profile.

### To modify an existing host profile:

- 1 On the mobile device, launch the Telnet Client.
- 2 From the Telnet Client **Options** menu, access the *Edit Host Profile* dialog box.
- 3 In the list of profiles in the *Edit Host Profile* dialog box, select the host profile dialog box that you want to modify.
- 4 Select `Edit`.
- 5 Use the *Edit Host Profile* dialog box to modify the basic parameters of the host profile (alias, IP address, TCP port number, and emulation type).
- 6 Select `More` to access and configure other emulation type-specific parameters for the host profiles.

---

**NOTE** For more information about the parameters in the *Edit Host Profile* dialog box and the parameters in the other emulation type-specific dialog boxes, see *Host Profile Settings* on page 201.

---

- 7 After you have modified the parameters for the host profile, select `Save`.

The changes that you have made are applied to the host profile. The *Edit Host Profile* dialog box closes and you return to the first *Edit Host Profile* dialog box.

- 8 Select `Done`.

The *Edit Host Profile* dialog box closes and you return to the primary Telnet Client interface

---

**NOTE** To exit either of the *Edit Host Profile* dialog boxes without saving the changes that you have made, press `Esc`.

---

## Deleting an Existing Host Profile

You can use the *Edit Host Profile* dialog box to delete an existing profile.

### To delete an existing host profile:

- 1 On the mobile device, launch the Telnet Client.
- 2 From the Telnet Client **Options** menu, access the *Edit Host Profile* dialog box.
- 3 From the list of host profiles in the *Edit Host Profile* dialog box, select the host profile that you want to delete.
- 4 Select `Delete`.

The host profile is deleted from the list of host profiles in the *Edit Host Profiles* dialog box.

- 5 Select `Done`.

The *Edit Host Profile* dialog box closes and you return to the primary Telnet Client interface.

---

**NOTE** To exit the *Edit Host Profile* dialog box without saving the changes that you have made, press `Esc`.

---

## Host Profile Settings

This section provides details about the configurable parameters that are available in the various host profile dialog boxes.

### Edit Host Profile Parameters

The following list describes the options and configurable parameters in the *Edit Host Profile* dialog box.

<b>Alias</b>	Indicates the name of the host profile. Usually, this is the name or alias of the host system with which the mobile device creates a Telnet session.  <b>Possible Values:</b> 1 - 50 alpha-numeric characters  <b>Default:</b> <None>
<b>Address</b>	Indicates the IP address or host name of the host system.  <b>Possible Values:</b> Any valid IP address, host name, or web address  <b>Default:</b> <None>
<b>Port</b>	Indicates the TCP port on which the host system is listening for Telnet connections.  <b>Possible Values:</b> 0 - 65535  <b>Default:</b> 23
<b>Emulation</b>	Indicates the type of emulation that the host system uses.  <b>Available Options:</b> <IBM-5251-11> <IBM-3278-2> <IBM-3279-2> <IBM-3279-2E> <VT100> <VT220> <HP> <WEB>  <b>Default:</b> <IBM-5251-11>
<b>Save</b>	Select this button to save the host profile and close the <i>Edit Host Profile</i> dialog box.

<b>More</b>	Select this button to access other, emulation type-specific parameters for the host profile.
<b>Config</b>	Select this button to modify the emulation parameters for the host profile.

### **More 5250 Options**

The *More 5250 Options* dialog box appears when the following criteria are met:

- You set the emulation type is to 5250 in the *Edit Host Profile* dialog box.
- You click `More` in the *Edit Host Profile* dialog box.

The following list describes the options and configurable parameters in the *More 5250 Options* dialog box.

**Device Name**

Indicates the workstation ID that mobile devices use to connect to the host system. This includes static characters and the following switches, which are used to capture dynamic data that is specific to each mobile device:

- **%a - %d.** Captures specific octets of the IP address of the mobile device. For example, use %a%b%c%d to capture all four IP octets of the address of the mobile device, or use %d to capture only the last octet of the IP address of the mobile device.
- **%m - %r.** Captures specific octets of the MAC address of the mobile device. (For example, use %p%q%r to capture the last three octets of the MAC address of the mobile device.)
- **%s.** Captures the session number.
- **%t.** Captures the Avalanche terminal ID of the mobile device. (If the mobile device is not an Avalanche client, this parameter is invalid.)

**Possible Values:** 1 - 20 alpha-numeric characters plus switches (see above)

**Default Value:** None

**NOTE:** IBM hosts usually truncate workstation IDs that are more than 10 characters. Also, the workstation ID should not begin with a numeric character.

**OK**

Select this button to save the changes that you have made and return to the *Edit Host Profile* dialog box.

**More VT Options**

The *More VT Options* dialog box appears when the following criteria are met:

- You have set the emulation type in the *Edit Host Profile* dialog box to VT100, VT220, or HP.
- You click `More` in selected in the *Edit Host Profile* dialog box.

The following list describes the options and configurable parameters in the *More VT Options* dialog box.

**Telnet Negotiation String** Indicates the Telnet negotiation string that the mobile device should use when establishing a Telnet session with the host system.

**Possible Values:** Any valid Telnet negotiation string

**Default:** <None>

**OK** Select this button to save the changes that you have made and return to the *Edit Host Profile* dialog box.

**Login** Select this button to access the *Edit AutoLogin* dialog box, which allows you to configure auto login parameters for the host connection.

### **Edit AutoLogin**

The *Edit AutoLogin* dialog box is accessed through the `Login` button in the *More VT Options* dialog box.

The following list describes the options and configurable parameters in the *Edit AutoLogin* dialog box.

**Name Prompt** Indicates the user name prompt that the host system uses.

**Possible Values:** Any valid user name prompt

**Default:** <None>

**Name** Indicates the user name that the mobile device supplies at the user name prompt.

**Possible Values:** Any valid user name

**Default:** <None>

<b>Password Prompt</b>	Indicates the password prompt that the host system uses.  <b>Possible Values:</b> Any valid password prompt  <b>Default:</b> <None>
<b>Password</b>	Indicates the password that the mobile device supplies at the password prompt.  <b>Possible Values:</b> Any valid user password  <b>Default:</b> <None>
<b>Command Prompt</b>	Indicates the command prompt that the host system uses.  <b>Possible Values:</b> Any valid command prompt  <b>Default:</b> <None>
<b>Command</b>	Indicates the command that the mobile device supplies at the command prompt.  <b>Possible Values:</b> Any valid command  <b>Default:</b> <None>
<b>OK</b>	Select this button to save the changes that you have made and return to the <i>More VT Options</i> dialog box.

## Manually Configuring Emulation Parameters

You can manually configure certain Telnet Client emulation parameters on a per-host basis.

---

**NOTE** For more information about global and per-host emulation parameters, see *Chapter 4: Emulation Parameters* on page 61.

---

---

**NOTE** You must use the Configuration Manager to modify most emulation parameters. For information about using Configuration Manager, see *Using Configuration Manager* on page 70.

---

## Accessing and Modifying Per-Host Emulation Parameters

You can manually modify certain per-host emulation parameters.

**To access and modify global emulation parameters:**

- 1 On the mobile device, launch the Telnet Client.
- 2 Access the Telnet Client **Options** menu.
- 3 From the Telnet Client Options menu, select `Configure > Emulation`.  
The *Input Password* dialog box appears.
- 4 In the **Input Terminal Config Password** text box, type the term config password.

---

**NOTE** The default Term Config password is “config”. For information modifying the Term Config password, see *Configuring Passwords* on page 235. If no Term Config password is configured, the Telnet Client will not prompt you for a password.

---

- 5 Select `OK`.

The *Select Host* dialog box appears.

- 6 In the *Select Host* dialog box, select the host profile that contains the emulation parameters that you want to modify.

- 7 Select `OK`.

The *Settings* dialog box appears for the host profile.

- 8 Use the various tabs in the *Settings* dialog box to modify the emulation parameters for the host profile.



---

**NOTE** For more information about the tabs and the configurable parameters in each tab of the *Settings* dialog box, see *Per-Host Emulation Parameters* on page 207.

---

- 9 After you have configured the emulation parameters for the host profile, select the **OK** button in the upper right corner of the *Settings* dialog box.

The *Settings* dialog box closes and you return to the primary Telnet Client interface.

## Per-Host Emulation Parameters

This section provides information about the parameters in the various tabs of the *Settings* dialog box.

### VTXX Settings

Use the VTXX tab in the *Settings* dialog box to configure parameters for VT-type emulation. If the host profile is configured for IBM-type emulation, you do not need to configure the VTXX tab.

The following list describes the parameters in the VTXX tab.

**Local Echo** Indicates whether the Telnet Client echoes characters that it received from a VT host.

**Possible Values:** <Enabled> <Disabled>

**Default:** <Disabled>

**8 Bit Control Codes** Indicates whether to use 8-bit ANSI control codes for VT-type emulation.

**Possible Values:** <Enabled> <Disabled>

**Default:** <Disabled>

**Backspace Sends Delete** Indicates whether the Telnet Client should send a delete control character when a user presses the backspace key.

**Possible Values:** <Enabled> <Disabled>

**Default:** <Disabled>

### **IBM Host Settings**

Use the IBM Host tab in the *Settings* dialog box to configure parameters for IBM-type emulation. If the host profile is configured for VT-type emulation, you do not need to configure the IBM Host tab.

The following table describes the configurable options in the IBM Host tab.

**5250 - Column Separator Dot** Indicates whether the Telnet Client displays a period or vertical line between each character when the host system uses a special column format mode.

**Possible Values:** <Enabled> <Disabled>

**Default:** <Enabled>

**5250 Swap Enter Key / Field Exit** Indicates whether the enter key is mapped to the field exit key and the clear key is mapped to the enter key.

**Possible Values:** <Enabled> <Disabled>

**Default:** <Disabled>

**3270 - Alternate System Request** Indicates whether the Telnet Client encodes 3270 system requests as requests instead of default interrupt processes.

**Possible Values:** <Enabled> <Disabled>

**Default:** <Disabled>

### **WEB Settings**

Use the WEB tab in the *Settings* dialog box to configure parameters for WEB emulation.

The following table describes the configurable options in the WEB tab.

**WEB Default Scanner Auto Keys** Determines the default post-scan action for web pages without Tab or Enter key META tags.

**Possible Values:** <No Keys> <Enter> <Tab> <Enter> and Tab>

**Default:** <No Keys>

**WEB Default Scanner State** Determines the default scanner state for web pages without scanner enabled/disabled META tags.

**Possible Values:** <Enabled> <Disabled> <Do Not Change>

**Default:** <Enabled>

<b>WEB Detect Out-Of-Range</b>	Indicates whether Telnet will prevent the user from interacting with a web page if the Wireless LAN adapter is not associated with an Access Point.  <b>Possible Values:</b> <Enabled> <Disabled>  <b>Default:</b> <Enabled>
<b>WEB Display Images</b>	Determines if embedded images and/or placeholders should be displayed on web pages.  <b>Possible Values:</b> <Enabled> <Disabled>  <b>Default:</b> <Enabled>
<b>WEB HTTP Version for Direct Connections</b>	Determines if the HTTP 1.0 or HTTP 1.1 protocol should be used for direct (non-proxy) connections.  <b>Possible Values:</b> <HTTP 1.0> <HTTP 1.1>  <b>Default:</b> <HTTP 1.1>
<b>WEB HTTP Version for Proxy Connections</b>	Determines if the HTTP 1.0 or HTTP 1.1 protocol should be used through proxy connections.  <b>Possible Values:</b> <HTTP 1.0> <HTTP 1.1>  <b>Default:</b> <HTTP 1.0>
<b>WEB Out-Of-Range Message</b>	Allows you to customize the out-of-range message that is displayed on the mobile device.  <b>Possible Values:</b> <Any>  <b>Default Message:</b> <Network Out Of Range>

**WEB Play Background Sounds** Determines whether sounds embedded in the web page will be played.

**Possible Values:** <No> <Yes>

**Default:** <Yes>

---

**NOTE** Sounds will only be played if supported by the mobile device sound card.

---

**WEB Underline Links** Determines if links (anchors) on the web page will be underlined.

**Possible Values:** <No> <Yes>

**Default:** <Yes>

---

**NOTE** This is not supported on Pocket PC and Windows Mobile devices.

---

**WEB User Agent** Specifies the value that is included with the HTTP header information sent by the device to the web server.

**Possible Values:** <Any valid User Agent value.>

**Default:** <The value that Internet Explorer or Pocket Internet Explorer would use on the device>

### **Message Settings**

Use the Message tab of the *Settings* dialog box to configure the settings for messages that the mobile device receives from the host system. Certain parameters in the Message tab are applicable only to 5250- and 3270-type emulation.

The following list describes the configurable options in the Message tab.

**Message Line  
(5250/3270 Only)**

Specifies the line from the host screen that the Telnet Client reads to display as the message line. The Telnet Client displays the message line each time its contents change. When the contents of the message line are not valid, the line appears in reverse video at the top of the display.

**Possible Values:** 0 - 24

**Default:** 24

**NOTE:** Use a value of 0 to prevent the display message.

**Auto Reset Delay  
(5250/3270 Only)**

Indicates the amount of time (in seconds) the Telnet Client waits before sending a reset to the host when the **Reset Required** parameter is set to `Never`.

**Possible Values:** 0 - 5 (seconds)

**Default:** 2

**Message Beeps  
(5250/3270 Only)**

Indicates the number of additional beeps that occur on the mobile device when the Telnet Client receives a system message.

**Possible Values:** Up to 255 characters, but only integer values are valid

**Default:** 0

**Reset Required  
(5250/3270 Only)**

Indicates the situations that require the user to press the reset key.

Options include:

- **On All Messages.** Requires a reset on screens that display information on line 24 (the bottom display line).
- **On Errors.** Requires a reset on screens that have an error indicator.
- **Never.** Requires the user to use a reset, but Telnet Client automatically performs the reset when it detects an error indicator.

**Possible Values:** <OnErrors> <On All Messages>  
<Never>

**Default:** <Disabled>

**Use Enter As Reset**

Indicates whether the enter key on the mobile device functions as the reset key when the mobile device is in an error state.

**Possible Values:** <Enabled> <Disabled>

**Default:** <Disabled>

**Font Settings**

Use the Font tab in the *Settings* dialog box to configure the way that text displays for the host connection.

The following list describes the configurable options in the Font tab.

<b>Name</b>	Indicates the font that the Telnet Client uses to display text in the emulation screen.  <b>Possible Values:</b> Any font installed on the mobile device  <b>Default Values:</b> <Courier New>
<b>Size</b>	Indicates the size (in points) in which text displays in the emulation screens.  <b>Possible Values:</b> 6 - 24  <b>Default Value:</b> 7
<b>Weight</b>	Indicates the weight that is applied to text in the emulation screens.  <b>Possible Values:</b> <Normal> <Bold>  <b>Default Value:</b> <Normal>
<b>Left (Clipping)</b>	Indicates the amount of white space (in font points) that the Telnet Client crops from the left of the font.  <b>Possible Values:</b> Up to 255 characters, but only integer values are valid  <b>Default Value:</b> 0
<b>Right (Clipping)</b>	Indicates the amount of white space (in font points) that the Telnet Client crops from the right of the font.  <b>Possible Values:</b> Up to 255 characters, but only integer values are valid  <b>Default Values:</b> 0



**Top (Clipping)** Indicates the amount of white space (in font points) that the Telnet Client crops from the top of the font.

**Possible Values:** Up to 255 characters, but only integer values are valid

**Default Values:** 0

**Bottom (Clipping)** Indicates the amount of white space (in font points) that the Telnet Client crops from the bottom of the font.

**Possible Values:** Up to 255 characters, but only integer values are valid

**Default Value:** 0

### **Display Settings**

Use the Display tab in the *Settings* dialog box to configure how the Telnet Client displays.

The following list describes the configurable options in the Display tab.

**Menu** Indicates whether the Telnet Client displays the Telnet Client menu during an active Telnet session.

**Possible Values:** <Enabled> <Disabled>

**Default Value:** <Enabled>

**Hide Menu (Button)** Click this button to access a dialog box that will allow you to configure a key sequence that will hide the Telnet Client menu during an active Telnet session.

**Hide Menu (Text Box)** Indicates the key sequence that is configured to hide the Telnet Client menu during an active Telnet session.

- Vertical Scrollbar** Indicates whether the Telnet Client displays the vertical scrollbar during a Telnet session.
- Possible Values:** <Enabled> <Disabled>
- Default Value:** <Disabled>
- Horizontal Scrollbar** Indicates whether the Telnet Client displays the horizontal scrollbar during a Telnet session.
- Possible Values:** <Enabled> <Disabled>
- Default Value:** <Disabled>
- Hide Keyboard (Button)** Click this button to access a dialog box that will allow you to configure a key sequence that hides/reveals the Telnet Client emulation keyboard.
- Hide Keyboard (Text Box)** Indicates the key sequence that is configured to hide/reveal the Telnet Client emulation keyboard.

### **View Settings**

Use the View tab in the *Settings* dialog box to configure how the view screen functions for the host connection.

The following list describes the configurable options in the View tab.

- Free Cursor** Indicates whether a user is allowed to move the cursor into “protected” areas of the screen.
- Possible Values:** <Enabled> <Disabled>
- Default Value:** <Enabled>
- Scrolling (Full Screen Mode)** Indicates whether the Telnet Client uses full-screen mode, which allows the user to scroll around the virtual display.
- Possible Values:** <Enabled> <Disabled>
- Default Value:** <Enabled>

- Scroll Offsets - Vert (Full-Screen Mode Only)** Specifies the number of columns that the vertical display moves when the cursor crosses the vertical edge of the screen.
- Possible Values:** 0 - 80
- Default Value:** 0
- NOTE:** Use 0 to indicate the current vertical display size.
- Scroll Offsets - Horz (Full-Screen Mode Only)** Specifies the number of rows that the virtual display moves when the cursor crosses the horizontal edge of the screen.
- Possible Values:** 0 - 24
- Default Value:** 0
- NOTE:** Use 0 to indicate the current horizontal display size.
- Fixed Screen Mode** Indicates whether the Telnet Client fixes the display on the mobile device to a specific position in the virtual display. When fixed-screen mode is enabled, the same portion of the virtual display appears on the display screen without regard to the location of the cursor.
- Possible Values:** <Enabled> <Disabled>
- Default Value:** <Disabled>
- NOTE:** If you enable fixed-screen mode, you must also specify the position in the **Fixed Screen Window Origin** group.

**Window Origin - Left  
(Fixed-Screen Mode  
Only)**

Specifies the virtual screen column where the display screen of the mobile device is fixed.

**Possible Values:** 1 - 79

**Default Value:** 1

**Window Origin - Top  
(Fixed-Screen Mode  
Only)**

Specifies the virtual screen row where the display screen of the mobile device is fixed.

**Possible Values:** 1 - 24

**Default Value:** 1

**Cursor Settings**

Use the Cursor tab in the *Settings* dialog box to configure the function of the cursor in emulation screens for the host connection.

The following list describes the configurable options in the Cursor tab.

**Cursor Edge Zones -  
Left**

Specifies the left border of the cursor zone in the virtual display. When the cursor moves outside of the border, the Telnet Client repositions the screen over the virtual display, centering the cursor on the display screen of the mobile device.

**Possible Values:** Up to 255 characters, but only integer values are valid

**Default Value:** 4

**Cursor Edge Zones -  
Right**

Specifies the right border of the cursor zone in the virtual display. When the cursor moves outside of the border, the Telnet Client repositions the screen over the virtual display, centering the cursor on the display screen of the mobile device.

**Possible Values:** Up to 255 characters, but only integer values are valid

**Default Value:** 1

<b>Tiling - Vert Mode</b>	<p>Determines how the Telnet Client handles vertical tiling. Options include:</p> <ul style="list-style-type: none"><li>• <b>None.</b> The Telnet Client repositions the screen on the cursor.</li><li>• <b>TopOnly:</b> The Telnet Client repositions the screen in the uppermost row of tiles.</li><li>• <b>All.</b> The Telnet Client always tiles vertically.</li></ul> <p><b>Possible Values:</b> &lt;All&gt; &lt;None&gt; &lt;TopOnly&gt;</p> <p><b>Default Value:</b> &lt;TopOnly&gt;</p>
<b>Tiling - Horz Mode</b>	<p>Determines how the Telnet Client handles horizontal tiling. Options include:</p> <ul style="list-style-type: none"><li>• <b>None.</b> The Telnet Client positions the screen around the cursor.</li><li>• <b>LeftOnly.</b> The Telnet Client positions the screen around the leftmost column of tiles.</li><li>• <b>All.</b> The Telnet Client always tiles horizontally.</li></ul> <p><b>Possible Values:</b> &lt;All&gt; &lt;LeftOnly&gt; &lt;None&gt;</p> <p><b>Default Value:</b> &lt;LeftOnly&gt;</p>
<b>Tiling - Vert</b>	<p>Specifies the height of the logical screen in “tiles” for tiling mode.</p> <p><b>Possible Values:</b> 0 - screen height (in rows)</p> <p><b>Default Value:</b> 0</p>
<b>Tiling - Horz</b>	<p>Specifies the width of the logical screen in “tiles” for tiling mode.</p> <p><b>Possible Values:</b> 0 - screen width (in rows)</p> <p><b>Default Value:</b> 0</p>

## Beeps Settings

Use the Beeps tab in the *Settings* dialog box to configure the beeps that the mobile device plays when it receives messages or errors from the host system.

The following list describes the configurable options in the Beeps tab.

### Message Beep

Indicates the sound that the mobile device generates when it receives a message from the host system.

**Possible Values:** <Default> <SystemAsterisk>  
<SystemExclamation> <SystemExit> <SystemHand>  
<SystemQuestion>

**Default Value:** <Default>

### Error Beep

Indicates the sound that the mobile device generates when it receives an error from the host system.

**Possible Values:** <Default> <SystemAsterisk>  
<SystemExclamation> <SystemExit> <SystemHand>  
<SystemQuestion>

**Default Value:** <Default>

### Silent Mode

Indicates whether silent mode is enabled. If silent mode is enabled, the mobile device will not play beeps when it receives messages or errors from the host system.

**Possible Values:** <Enabled> <Disabled>

**Default Value:** <Disabled>

### Test

Tests the beep settings that are configured. The mobile device will play the beeps that are configured for messages and errors, in that order.

## Telnet Settings

Use the Telnet tab in the *Settings* dialog box to configure the Telnet auto-connect feature for connections to the host system.

The following list describes the configurable options in the Telnet tab.

**Auto Connect** Indicates whether the mobile device should attempt to reconnect to the host system when the host system terminates the session.

**Possible Values:** <Enabled> <Disabled>

**Default Value:** <Disabled>

### Printer Settings

Use the Printer tab in the *Settings* dialog box to configure the printer that the mobile device is using for the host connection.

The following list describes the options and configurable parameters in the Printer tab.

**Printer** Indicates the printer that the mobile device uses.

**Possible Values:** <PS1000> <PS1001> <PS1004>  
<LINEPRINTER> <DUMB> <COMTEC>  
<PATHFINDER> <RASCAL> <RENEGADE>  
<COMTECL\_PS> <CODE\_COURIER>  
<COMTEC\_RF> <COMTEC\_RF\_960> <TEC> <User  
Defined>

**Default Value:** <PS1000>

**Port** Indicates the COM port on the mobile device to which the printer is connected.

**Possible Values:** <COM1>

**Default Value:** <COM1>

**Baud** Indicates the baud rate of the serial connection to the printer.

**Possible Values:** <9600> <14400> <19200> <38400>  
<57600> <115200>

**Default Value:** <9600>

---

<b>Parity</b>	<p>Indicates the parity of the serial connection to the printer.</p> <p>Possible Values: &lt;None&gt; &lt;Even&gt; &lt;Mark&gt; &lt;Odd&gt; &lt;Space&gt;</p> <p>Default Value: &lt;None&gt;</p>
<b>Data</b>	<p>Indicates the data bits (the number of bits in each octet) of the serial connection to the printer.</p> <p><b>Possible Values:</b> &lt;4&gt; &lt;5&gt; &lt;6&gt; &lt;7&gt; &lt;8&gt;</p> <p><b>Default Value:</b> &lt;8&gt;</p>
<b>Stop</b>	<p>Indicates the number of stop bits that the serial connection to the printer uses.</p> <p><b>Possible Values:</b> &lt;1&gt; &lt;2&gt;</p> <p><b>Default Value:</b> &lt;1&gt;</p>
<b>Wakeup</b>	<p>Indicates the string of characters that the mobile device sends to the printer as a wakeup. You can represent the wakeup string as an ASCII or hex value.</p> <ul style="list-style-type: none"><li>• <b>Hex Value.</b> Type the hex values of the characters that you want the mobile device to send to the printer. For example, 0000 sends two nulls to the printer.</li><li>• <b>ASCII Value.</b> Use "&lt;&gt;" to enclose ASCII hex values. For example, &lt;00&gt; &lt;00&gt; sends two nulls to the printer.</li></ul> <p><b>Possible Values:</b> Any valid wakeup string</p> <p><b>Default Value:</b> &lt;None&gt;</p>



**Hardware Flow Control** Indicates whether the serial connection to the printer uses hardware flow control.

**Possible Values:** <Enabled> <Disabled>

**Default Value:** <Disabled>

**Software Flow Control** Indicates whether the serial connection to the printer uses software flow control.

**Possible Values:** <Enabled> <Disabled>

**Default Value:** <Disabled>



## Appendix A: Using Microsoft ActiveSync

This section provides information about creating Microsoft ActiveSync connections between host systems and mobile devices.

### Requirements

Before you create a Microsoft ActiveSync partnership, ensure that you have the following:

- Microsoft ActiveSync 3.7 (or better) installed on the host system
- Serial cable or USB cable to connect the host system to the mobile device
- Device cradle for the mobile device

### Overview of Creating a Partnership

Creating a partnership involves the following tasks:

- Selecting the Microsoft ActiveSync Connection Method on the Mobile Device.
- Selecting the Microsoft ActiveSync Method on the Host System.
- Freeing a COM Port.
- Creating a Partnership.

### Selecting the Microsoft ActiveSync Connection Method on the Mobile Device

Most mobile devices allow Microsoft ActiveSync connections over a serial or USB connection. Before you can establish a Microsoft ActiveSync partnership, you must select the connection method (serial or USB) on the mobile device.

**To select the Microsoft ActiveSync connection method on the mobile device:**

- 1 On the mobile device, launch Microsoft ActiveSync.
- 2 From the Microsoft ActiveSync **Tools** menu, select `Options`.

---

**NOTE** The `Options` option is only available when the mobile device is not engaged in an active partnership with a host system.

---

The *PC Synchronization* dialog box appears.

**3** In the `PC` tab of the *PC Synchronization* dialog box, enable the **Sync with this PC during manual sync** checkbox.

**4** Click `Options...`

The *PC Synchronization Options* dialog box appears.

**5** Enable the **Enable PC sync using this connection** checkbox.

**6** From the **Enable PC sync using this connection** menu list, select the connection method.

- If you are using a USB cable to connect the host system and the mobile device, then select `USB Default`.
- If you are using a serial cable to connect the host system and the mobile device, select the appropriate baud rate.

**7** Click `OK`.

The *PC Synchronization Options* dialog box closes.

**8** Click `OK`.

The *PC Synchronization* dialog box closes and you are returned to the Microsoft ActiveSync interface.

The mobile device is now configured with the correct synchronization method.

## Selecting the Microsoft ActiveSync Method on the Host System

Use the Microsoft ActiveSync interface on the host system to configure the connection method (USB or serial).

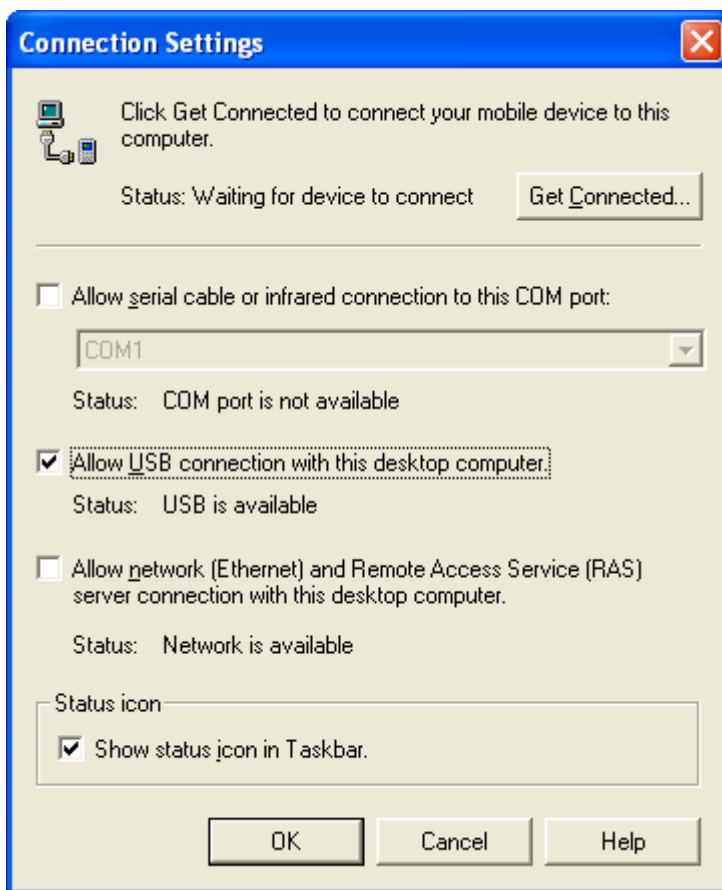
**To configure the connection method on the host system:**

- 1 On the host system, launch Microsoft ActiveSync.
- 2 From the Microsoft ActiveSync **File** menu, select *Connection Settings...*

The *Connection Settings* dialog box appears.

- 3 Use the *Connection Settings* dialog box to configure the connection method between the host system and the mobile device:
  - If you are using a USB connection, then enable the **Allow USB connection with this desktop computer** checkbox.
  - If you are using a serial connection, then enable the **Allow serial or infrared connection to this COM port** checkbox, and then use the corresponding menu list to select the COM port that you are using.

The following figure provides an example.



**Figure A-1.** *Selecting the Connection Method on the Host System*

**4** Click **OK**.

The *Connection Settings* dialog box closes and you are returned to the Microsoft ActiveSync interface.

The host system is now configured with the correct Microsoft ActiveSync connection method.

## Freeing a COM Port

If you are using a serial cable to connect the host system and the mobile device, you may need to ensure that the COM port to which you connect the serial cable is available for Microsoft ActiveSync to use.

Applications, including Microsoft ActiveSync, contend for “ownership” or exclusive use of the COM ports on the host system. Before you attempt to create a partnership, ensure that no other applications are using the COM port through which you will establish the partnership with the mobile device.

To free the COM port for Microsoft ActiveSync, shut down the application or stop the service that has control of the COM port.

For example, if you have installed Avalanche Manager on the host system and have used Avalanche Manager to perform serial updates on the mobile device, then Avalanche Manager may have exclusive control of the COM ports on the host system. To free the COM port(s), access the Services administrative tool on the host system and stop the Wavelink Avalanche Manager service.

## Creating a Partnership

Microsoft ActiveSync uses two types of partnerships:

- **Standard.** A standard partnership allows you to synchronize data (for example, scheduling information) between the host system and the mobile device. Additionally, when you create a standard partnership, you do not have to recreate the partnership each time you reconnect the host system and the mobile device, which is the case with guest partnerships.
- **Guest.** A guest partnership does not synchronize data between the host system and the mobile device, but it requires less setup time than a standard partnership. However, because no synchronization takes place, you must re-establish a partnership each time you reconnect the host system and the mobile device.

You may use either a standard or guest partnership to install the Telnet Client and to download Telnet Client configurations to the mobile device.

## Creating a Standard Partnership

You may use a standard partnership to install the Telnet Client and download Telnet Client configurations to the mobile device.

A standard partnership synchronizes data and settings between the host system and the mobile device.

### To create a standard Microsoft ActiveSync partnership:

- 1 Connect the mobile device to the host system with a serial or USB cable.
- 2 On the mobile device, ensure that you have selected the correct connection method.

---

**NOTE** For more information about selecting the connection method, see *Selecting the Microsoft ActiveSync Connection Method on the Mobile Device* on page 225.

---

- 3 On the host system, ensure that you have enabled the correct connection method.

---

**NOTE** For more information about configuring the connection method on the host system, see *Selecting the Microsoft ActiveSync Method on the Host System* on page 226.

---

- 4 If you are using a serial port to connect to the mobile device, ensure that the serial port on the host system is free for Microsoft ActiveSync to use.

---

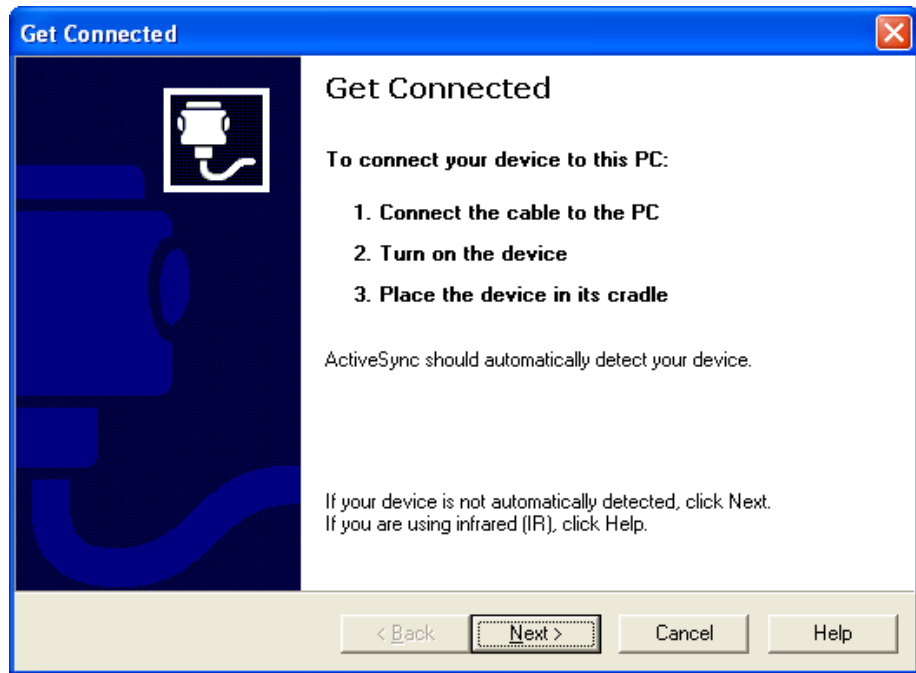
**NOTE** For more information about freeing a COM port on the host system, see *Freeing a COM Port* on page 229.

---

- 5 On the host system, launch Microsoft ActiveSync.
- 6 From the Microsoft ActiveSync **File** menu, select `Get Connected...`

The *Get Connected* dialog box appears.





**Figure A-2.** *Get Connected Dialog Box*

**7** Click *Next*.

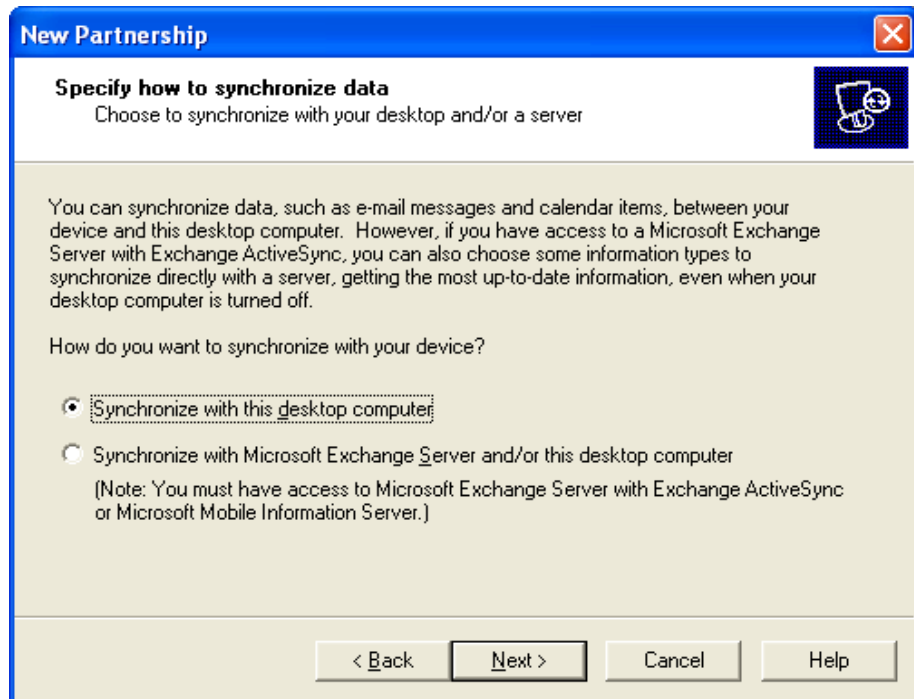
Microsoft ActiveSync attempts to communicate with the mobile device.

Once Microsoft ActiveSync establishes a connection with the mobile device, the *New Partnership* dialog box appears.

**8** In the *New Partnership* dialog box, enable the **Standard Partnership** option.

**9** Click *Next*.

The *Specify how to synchronize data* dialog box appears.



**Figure A-3.** *Select Synchronization Settings Dialog Box*

- 10** In the *Specify How to Synchronize Data* dialog box, enable the synchronization option that you want to use.
- 11** Click `Next`.

The *Select Synchronization Settings* dialog box appears.

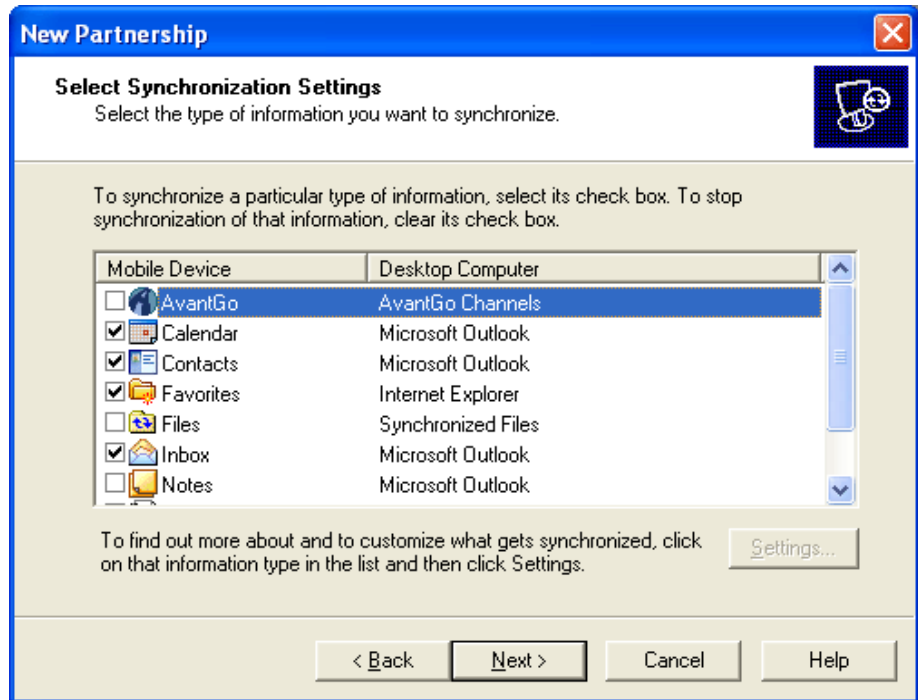
- 12** In the *Select Synchronization Settings* dialog box, enable the checkboxes the components that you want to synchronize between the host system and the mobile device.

---

**NOTE** You do not have to synchronize any data types to install the Telnet Client and download Telnet Client configurations to the mobile device.

---

The following figure shows the *Select Synchronization Settings* dialog box.



**Figure A-4.** *Selecting the Components to Synchronize*

**13** Click **Next**.

The *Setup Complete* dialog box appears.

**14** Click **Finish**.

Microsoft ActiveSync indicates that the mobile device and the host system are connected and synchronized.



**Figure A-5.** *Host System and Mobile Device Are Synchronized*

The standard partnership is complete. You are now able to disconnect and re-connect the mobile device to the host system without having to re-create the partnership.

## Creating a Guest Partnership

You may use a guest partnership to install the Telnet Client and download Telnet Client configurations to the mobile device.

### To create a guest partnership:

- 1 Connect the mobile device to the host system with a serial or USB cable.
- 2 On the mobile device, ensure that you have selected the correct connection method.

---

**NOTE** For more information about selecting the connection method, see *Selecting the Microsoft ActiveSync Connection Method on the Mobile Device* on page 225.

---

- 3 On the host system ensure that you have selected the correct connection method.

---

**NOTE** For more information about configuring the correct connection method on the host system, see *Selecting the Microsoft ActiveSync Method on the Host System* on page 226.

---

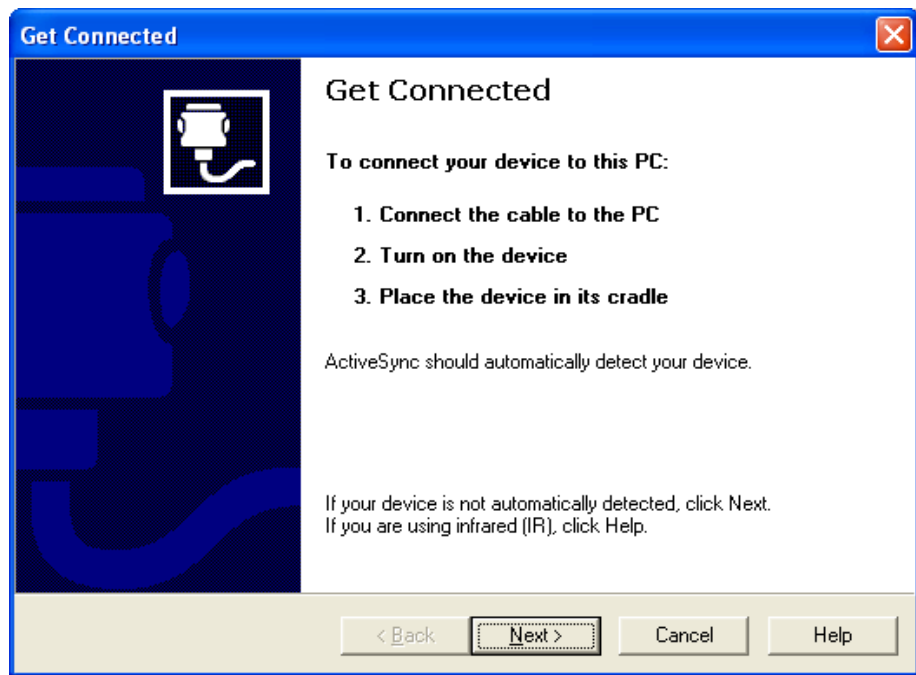
- 4 If you are using a serial port to connect to the mobile device, ensure that the serial port on the host system is free for Microsoft ActiveSync to use.

---

**NOTE** For more information about freeing a COM port on the host system, see *Freeing a COM Port* on page 229.

---

- 5 On the host system, launch Microsoft ActiveSync.
- 6 From the Microsoft ActiveSync **File** menu, select *Get Connected...*  
The *Get Connected* dialog box appears.



**Figure A-6.** *Get Connected Dialog Box*

**7** Click *Next*.

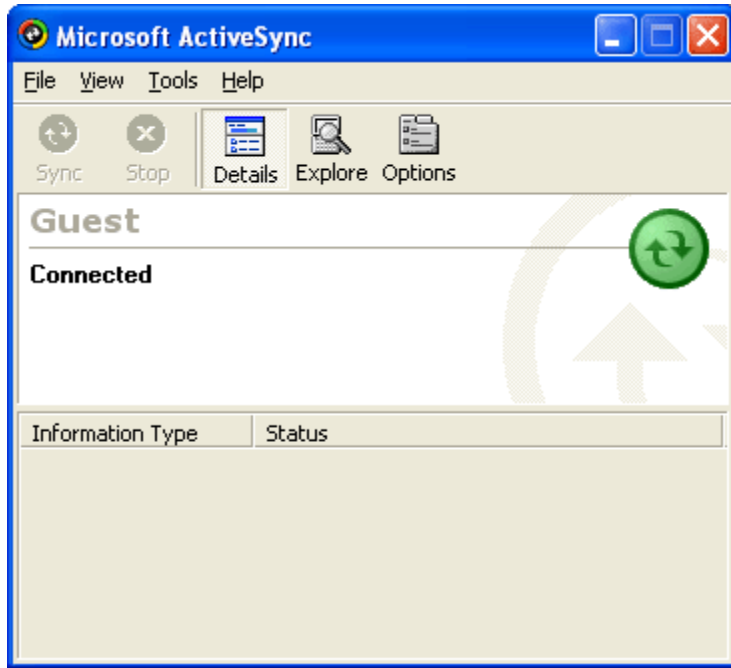
Microsoft ActiveSync attempts to communicate with the mobile device.

Once Microsoft ActiveSync establishes a connection with the mobile device, the *New Partnership* dialog box appears.

**8** In the *New Partnership* dialog box, select the **Guest Partnership** option.

**9** Click *Next*.

Microsoft ActiveSync indicates that the guest partnership has been created.



**Figure A-7.** Microsoft ActiveSync Guest Partnership





## Appendix B: Common Configuration Tasks

This section provides information about where to locate and configure common parameters for the Telnet Client, including:

- Configuring Passwords
- Configuring the Number of Concurrent Sessions
- Configuring IP Printing
- Configuring License Server IP Address
- Configuring Telnet Client Display Settings
- Configuring Telnet Client Lockdown
- Configuring Key Macros
- Configuring Screen Panning
- Configuring ActiveText
- Configuring Scan Handlers
- Configuring Autologin for VT Emulation
- Configuring Telnet Negotiation Strings for VT Emulation
- Configuring Workstation IDs for 5250/3270 Emulation
- Enabling Battery Strength and Signal Strength Icons

### Configuring Passwords

Certain components of the Telnet Client are password protected. Users at the mobile device must supply a password to perform the following functions:

- Manually configure host profiles
- Manually configure per-host emulation parameters
- Exit the Telnet Client

---

**NOTE** By default, an exit password is not configured. If an exit password is not configured, users are not prompted for a password when they choose to exit the Telnet Client application.

---

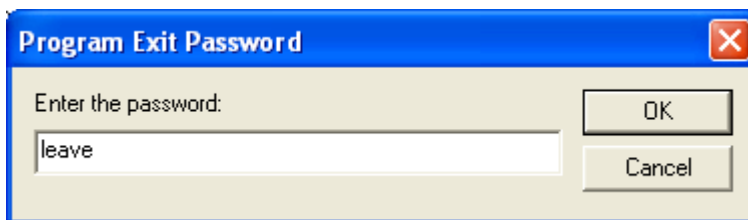
The following table provides information about and describes where each of these parameters can be configured in host profiles.

Function	Location in Configuration Manager	Parameter Name	Default Setting
Configure Host Profiles	Emulation > Common	RF Config Password	SYSTEM
Configure Per-Host Emulation Parameters	Emulation > Common	Term Config Password	CONFIG
Exit Telnet Client	Emulation > Common	Program Exit Password	<None>

**Table B-1:** *Configuring Telnet Client Passwords*

**To configure a password:**

- 1 Access the Configuration Manager.
- 2 In the Configuration Manager, locate the password parameter (see Table B-1) that you want to modify.
- 3 Use the dialog box for the password parameter to configure the password.



**Figure B-1.** *Configuring the Terminal Configuration Passwords*

- 4 Click **OK**.
- 5 Save the new configuration.

- 6 Close the Configuration Manager and download the new configuration to the mobile device.

---

**NOTE** For more information about using the Configuration Manager, see *Chapter 4: Emulation Parameters* on page 61.

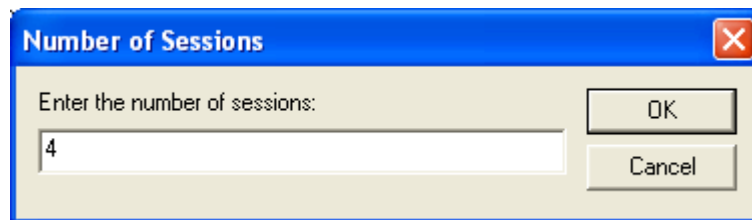
---

## Configuring the Number of Concurrent Sessions

The Telnet Client allows up to four concurrent Telnet sessions. However, by default, the Telnet Client is configured to allow a user to initiate and maintain one session. Use the Configuration Manager to specify the number of concurrent Telnet sessions that the Telnet Client should support.

**To modify the maximum number of concurrent sessions:**

- 1 Access the Configuration Manager.
- 2 Locate the `Emulation > Common > Number of Sessions` parameter.
- 3 Use the *Number of Sessions* dialog box to specify the maximum number of sessions.



**Figure B-2.** *Modifying the Maximum Number of Concurrent Sessions*

- 4 Click `OK`.
- 5 Save the new configuration.
- 6 Close the Configuration Manager and download the new configuration to the mobile device.

---

**NOTE** For more information about using the Configuration Manager, see *Chapter 4: Emulation Parameters* on page 61.

---

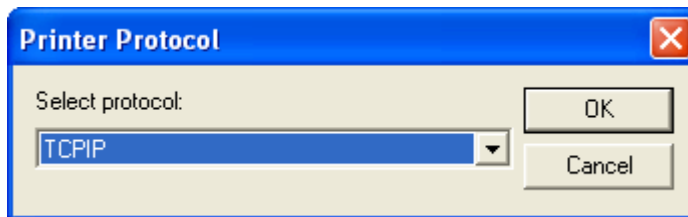
## Configuring IP Printing

Most mobile devices do not use a printer that is directly connected. Instead, mobile devices print over the network via IP.

Use the Configuration Manager to configure mobile devices for IP printing.

### To configure the Telnet Client for IP printing:

- 1 Access the Configuration Manager.
- 2 In the Configuration Manager, locate the `Emulation > Printing > Printer Protocol` parameter.
- 3 In the *Printer Protocol* dialog box, select `TCPIP`.



**Figure B-3.** *Configuring Mobile Devices for IP Printing*

- 4 Click `OK`.
- 5 Save the new configuration.
- 6 Close the Configuration Manager and download the new configuration to the mobile device.

---

**NOTE** For more information about using the Configuration Manager, see *Chapter 4: Emulation Parameters* on page 61.

---

## Configuring License Server IP Address

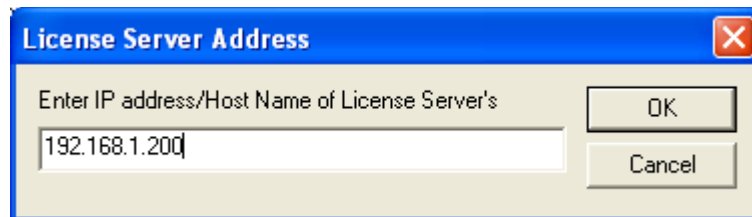
The Telnet Client requires a valid license for full functionality. You can configure a license at the mobile device manually, or you can configure the client to obtain a license from a license server on the network.

A mobile device will automatically find the license server on the local IP subnet. However, if your license server is located on another subnet, you will need to configure the mobile device with the IP address of the license server.

Use the Configuration Manager to configure the license server IP address.

### To configure the IP address of a remote license server:

- 1 Access the Configuration Manager.
- 2 In the Configuration Manager, locate the Emulation > Common > License Server Address parameter.
- 3 Use the *License Server Address* dialog box to configure the IP address of the license server.



**Figure B-4.** Configuring the License Server IP Address

- 4 Click OK.
- 5 Save the new configuration.
- 6 Close the Configuration Manager and download the new configuration to the mobile device.

---

**NOTE** For more information about using the Configuration Manager, see *Chapter 4: Emulation Parameters* on page 61.

---

## Configuring Telnet Client Display Settings

You can modify and customize the way that the Telnet Client displays, including:

- Whether the Windows Start menu displays while the Telnet Client is active.
- Whether the Telnet Client menu displays while the Telnet Client is engaged in a Telnet session.
- Whether the vertical or horizontal scrollbars display during an active Telnet session.

Use the Configuration Manager to customize these (and other) display features of the Telnet Client.

Table B-2 provides a list of display options and the parameters (in the Configuration Manager) that are used to customize these options.

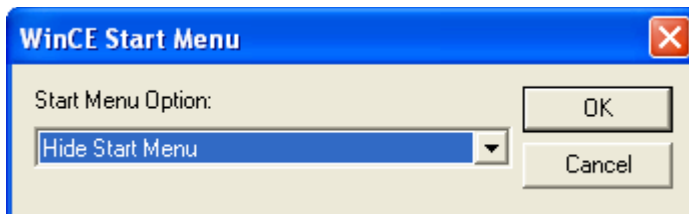
Display Option	Location in the Configuration Manager	Parameter Name	Default Setting
Hide Windows Start Menu	Emulation > Display	WinCE Hide Start Menu	<Show Standard Start Menu>
Hide Telnet Client Menu	Emulation > Display	WinCE Hide Menu	<No>
Hide the Telnet Client Vertical Scrollbar	Emulation > Display	WinCE Hide Vertical Scrollbar	<Yes>
Hide the Telnet Client Horizontal Scrollbar	Emulation > Display	WinCE Hide Horizontal Scrollbar	<Yes>
Create a Key Sequence to Hide/Reveal the Telnet Client command bar	Emulation > Display	WinCE Menu Toggle Key	<Default> (No key sequence configured)
Specify the Font that Emulation Uses	Emulation > Display	WinCE Font Name	<Standard>
Specify the Font Size that Emulation Uses	Emulation > Display	WinCE Font Size	<7>

**Table B-2:** Customizing the Telnet Client Display

### To configure a display setting:

- 1 Access the Configuration Manager.

- 2 In the Configuration Manager, locate the display option that you want to modify (see Table B-2).
- 3 Use the dialog box for the parameter to configure the display option.



**Figure B-5.** *Configuring the Telnet Client to Hide the Windows Start Menu*

- 4 Click **OK**.
- 5 Save the new configuration.
- 6 Close the Configuration Manager and download the new configuration to the mobile device.

---

**NOTE** For more information about using the Configuration Manager, see *Chapter 4: Emulation Parameters* on page 61.

---

## Configuring Telnet Client Lockdown

You can configure several Telnet Client parameters to effectively lockdown the Telnet Client and prevent users at the mobile device from launching other applications on the mobile device.

---

**NOTE** When you configure Telnet Client lockdown, record your passwords and key sequences in a secure location for administrative purposes. By configuring lockdown, you can effectively lock yourself out of the mobile device. If you forget the passwords that you have configured, you will be required to reboot the system and reconfigure the Telnet Client.

---

Use the Configuration Manager to lockdown the mobile device.

Table B-3 lists the parameters in the Configuration Manager that you must use to effectively lockdown the Telnet Client.

Parameter to Modify	Location in the Configuration Manager	Parameter Setting
WinCE Hide Start Menu	Emulation > Display	<Hide Start Menu>
WinCE Hide Menu*	Emulation > Display	<Yes>
WinCE Menu Toggle Key*	Emulation > Display	Do not configure a toggle key (by default, no toggle key is configured)
RF Config Password	Emulation > Common	Configure a secure password
Term Config Password	Emulation > Common	Configure a secure password
Program Exit Password	Emulation > Common	Configure a secure password
Program Exit Key	Emulation > Common	Configure an exit key
* Hiding and preventing access to the Telnet Client is not mandatory to locking down the Telnet Client, but provides an additional layer of security.		

**Table B-3:** *Configuring Telnet Client Lockdown*

**To configure Telnet Client lockdown:**

- 1 Access the Configuration Manager.
- 2 In the Configuration Manager, modify the lockdown parameters (see Table B-3).



**Figure B-6.** *Configuring One of the Parameters for Lockdown*

- 3 Save the new configuration.
- 4 Close the Configuration Manager and download the new configuration to the mobile device.



---

**NOTE** For more information about using the Configuration Manager, see *Chapter 4: Emulation Parameters* on page 61.

---

## Configuring Key Macros

Use the Configuration Manager to create, configure, or remove key macros for emulation.

### To configure a key macro:

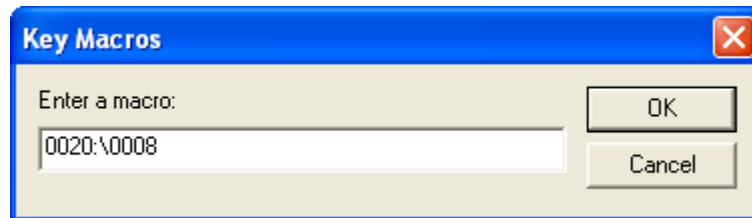
- 1 Access the Configuration Manager.
- 2 In the Configuration Manager, locate and right-click the `Emulation > Common > Key Macro` parameter.

A menu list appears.

- 3 From the menu list, select `Add`.

The *Key Macros* dialog box appears.

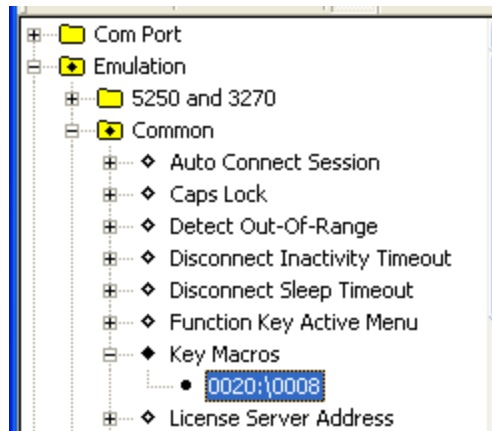
- 4 Use the *Key Macros* dialog box to configure the new key macro.



**Figure B-7.** *Configuring a Key Macro*

- 5 After you have configured the key macro, click `OK`.

The new key macro now appears beneath the `Key Macros` parameters in the Configuration Manager.



**Figure B-8.** Key Macro in Configuration Manager

- 6 Save the new configuration.
- 7 Close the Configuration Manager.
- 8 Download the new configuration to the mobile device.

---

**NOTE** For more information about modifying configuration parameters and using the Configuration Manager, see *Chapter 4: Emulation Parameters* on page 61.

---

## Configuring Screen Panning

Use the Configuration Manager to configure Telnet Client screen panning.

The screen panning feature of the Telnet Client allows a user to scroll around the screen by tapping and dragging the stylus. By default, screen panning is enabled on the Telnet Client.

Screen panning has two methods of operation:

- Standard
- Reversed

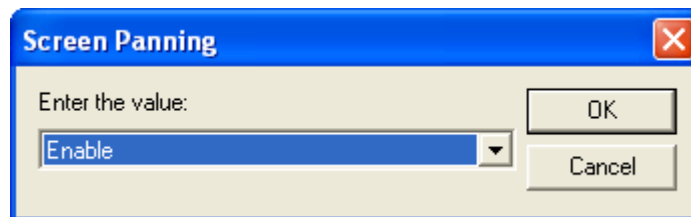
If you want to use reverse screen panning, you must enable standard screen panning.

**To configure screen panning:**

- 1 Access the Configuration Manager.
- 2 In the Configuration Manager, locate and right-click `Emulation > Display > Screen Panning`.

The *Screen Panning* dialog box appears.

- 3 Use the *Screen Panning* dialog box to enable or disable screen panning for the Telnet Client.



**Figure B-9.** *Configuring Screen Panning*

- 4 Click `OK`.
- 5 If you want to enable/disable reverse screen panning, locate and right-click `Emulation > Display > Screen Panning Reversed` parameters.  
  
The *Screen Panning Reversed* dialog box appears.
- 6 Use the *Screen Panning Reversed* dialog box to enable or disable reverse screen panning.

---

**NOTE** For reverse screen panning to work, you must also enable screen panning.

---

- 7 Click `OK`.
- 8 Save the new configuration.
- 9 Close the Configuration Manager.

**10** Download the new configuration to the mobile device.

---

**NOTE** For more information about modifying configuration parameters and using the Configuration Manager, see *Chapter 4: Emulation Parameters* on page 61.

---

## Configuring ActiveText

Use the Configuration Manager to configure the ActiveText feature of the Telnet Client.

The ActiveText feature of the Telnet Client identifies certain strings of text and converts them to objects that a user can select-and-click.

The ActiveText feature can identify two types of strings:

- Simple menu item
- AS/400-style function key

By default, both types of ActiveText are enabled on the Telnet Client.

Table B-4 indicates the parameters in Configuration Manager that control the different types of ActiveText.

ActiveText Type	Configuration Manager Parameter
Simple Menu Item	Emulation > Common > Simple Number Menu Active Text
AS/400-Style Function Key	Emulation > Common > Function Key Active Menu

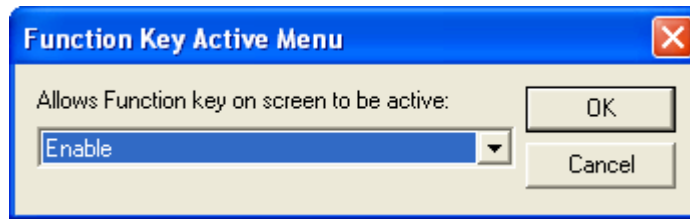
**Table B-4:** *ActiveText Parameters in Configuration Manager*

### To configure ActiveText:

- 1** Access the Configuration Manager.
- 2** In the Configuration Manager, locate and right-click the parameter for the type of ActiveText that you want to configure (see Table B-4).

A dialog box for the ActiveText type appears.

- 3** Use the dialog box to enable or disable the ActiveText.



**Figure B-10.** *Configuring ActiveText*

- 4 Click **OK**.
- 5 Save the new configuration.
- 6 Close the Configuration Manager.
- 7 Download the new configuration to the mobile device.

---

**NOTE** For more information about modifying configuration parameters and using the Configuration Manager, see *Chapter 4: Emulation Parameters* on page 61.

---

## Configuring Scan Handlers

Use the Configuration Manager to configure scan handlers.

Scan handlers allow you to define special functions that are applied to the processing of a scan. A scan handler allows you to strip data from the beginning or end of a scan and/or to replace certain characters within a scan.

### To configure a scan handler:

- 1 Access the Configuration Manager.
- 2 In Configuration Manager, locate and right-click the `Scanner > Common > Scan Handler` parameter.

A menu list appears.

- 3 Click `Add`.

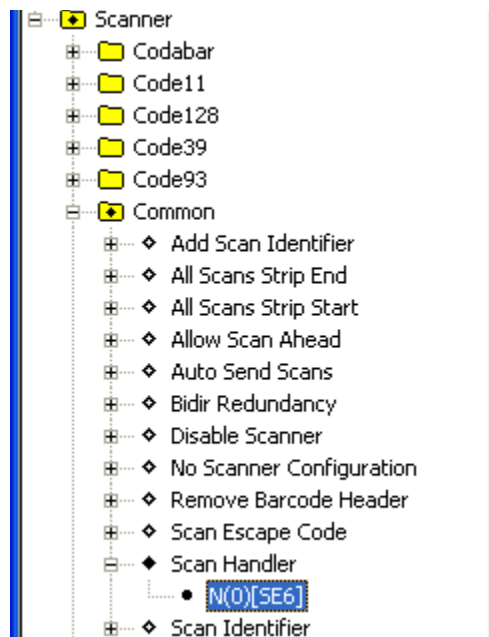
The *Scan Handler* dialog box appears.

- 4 Use the *Scan Handler* dialog box to configure a new scan handler.



**Figure B-11.** *Configuring a Scan Handler*

- 5 Click **OK**.
- 6 The new scan handler now appears beneath the **Scan Handler** parameter in the Configuration Manager.



**Figure B-12.** *Scan Handler in the Configuration Manager*

- 7 Save the new configuration.
- 8 Close the Configuration Manager.

- 9 Download the new configuration to the mobile device.

---

**NOTE** For more information about modifying configuration parameters and using the Configuration Manager, see *Chapter 4: Emulation Parameters* on page 61.

---

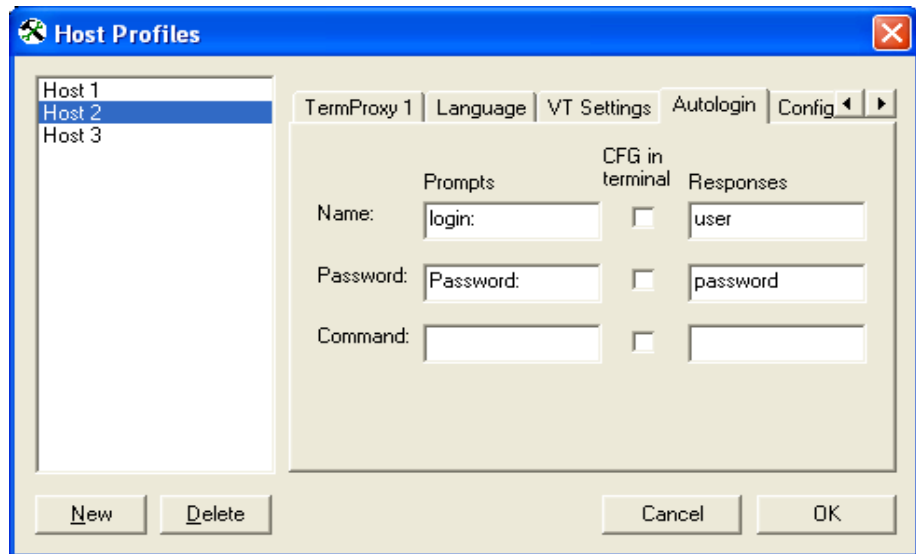
## Configuring Autologin for VT Emulation

You can configure the mobile device to send automatic responses to prompts from a host. This allows for automatic login for VT/HP emulation.

Because autologin is specific to each host system, autologin is configured in the *Host Profiles* dialog box.

### To configure a mobile device for automatic login to a host:

- 1 Access the *Host Profiles* dialog box.
- 2 From the list of host profiles in the *Host Profiles* dialog box, select the host for which you want to configure autologin parameters.
- 3 Ensure that you have selected a VT-type or HP emulation type from the **Emulation** drop-down menu in the Host tab of the *Host Profiles* dialog box. (If you have not selected VT/HP emulation, you will not be able to configure a autologin.)
- 4 Select the Autologin tab.
- 5 Configure the Autologin tab.



**Figure B-13.** *Configuring VT Autologin*

---

**NOTE** For information about the parameters in the Autologin tab, see *Chapter 3: Host Profiles* on page 29.

---

- 6 After you have configured the Autologin tab, click **OK**.
- 7 Download the new configuration to the mobile device.

---

**NOTE** For more information about configuring host profiles, see *Chapter 3: Host Profiles* on page 29.

---

## Configuring Telnet Negotiation Strings for VT Emulation

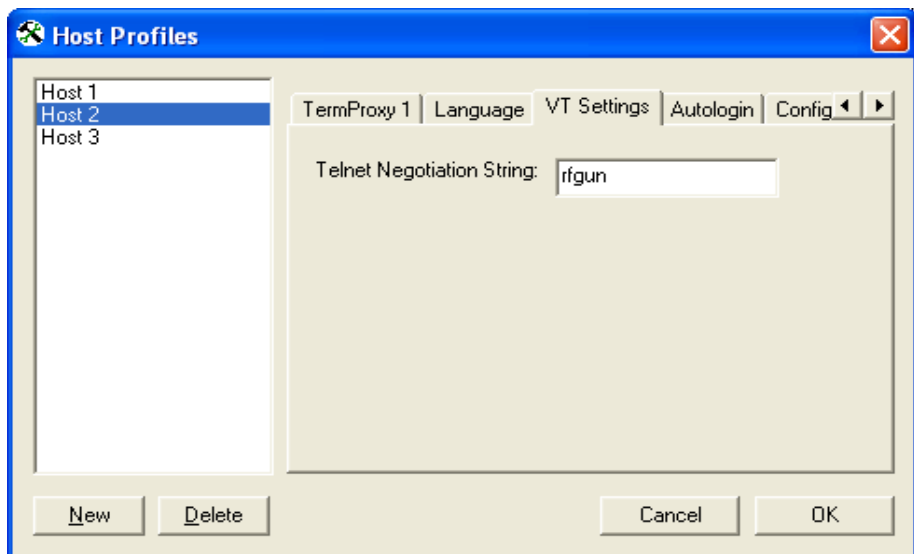
A Telnet negotiation string is used to identify a mobile device to a host system and to present a client with the appropriate emulation options.

Because Telnet negotiation strings are host specific, they are configured in the *Host Profiles* dialog box.



**To configure a Telnet negotiation string:**

- 1 Access the *Host Profiles* dialog box.
- 2 From the list of host profiles in the *Host Profiles* dialog box, select the host for which you want to configure the Telnet negotiation string.
- 3 Ensure that you have selected a VT-type or HP emulation type from the **Type** drop-down list in the Host tab of the *Host Profiles* dialog box. (If you have not selected VT/HP emulation, you will not be able to configure a Telnet negotiation string.)
- 4 In the *Host Profiles* dialog box, select the VT Settings tab.
- 5 In the **Telnet Negotiation String** text box, configure the Telnet negotiation string that the mobile device should use when connecting to the host system.



**Figure B-14.** *Configuring a Telnet Negotiation String*

- 6 Click **OK**.
- 7 Download the new configuration to the mobile device.

---

**NOTE** For more information about configuring host profiles, see *Chapter 3: Host Profiles* on page 29.

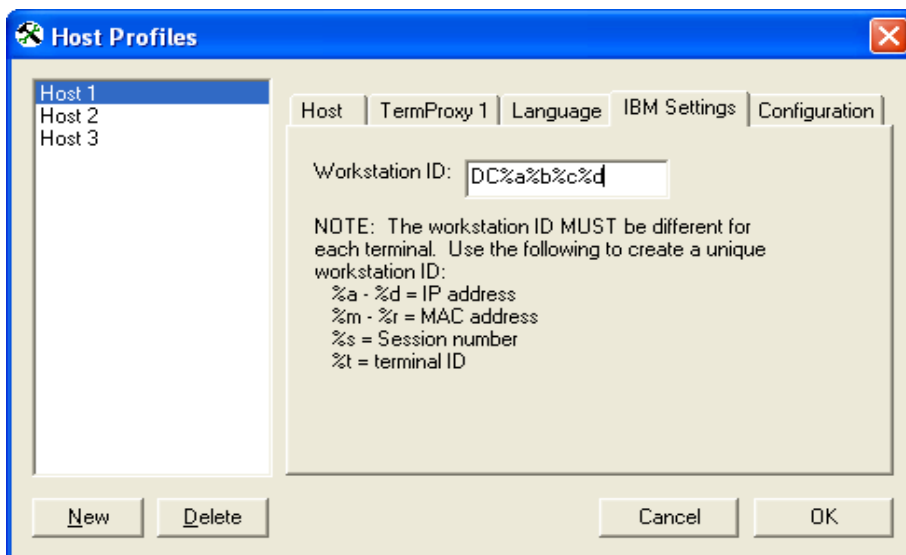
---

## Configuring Workstation IDs for 5250/3270 Emulation

The Telnet Client allows you to dynamically generate a workstation ID for a mobile device. Because workstation IDs are specific to each host connection, workstation IDs are configured in the *Host Profiles* dialog box.

### To configure the Telnet Client to dynamically generate a workstation ID:

- 1 Access the *Host Profiles* dialog box.
- 2 From the list of host profiles in the *Host Profiles* dialog box, select the host connection for which you want to configure a workstation ID.
- 3 Ensure that you have selected 5250/3270 emulation from the **Type** drop-down list in the Host tab. (If you have not selected a 5250/3270 emulation type, you will not be able to configure a workstation ID.)
- 4 Select the IBM Settings tab.
- 5 Use the **Workstation ID** text box to configure the dynamic generation of a workstation ID for mobile devices that use the host profile.



**Figure B-15.** *Configuring the Workstation ID*

- 6 Click **OK**.

The new configuration is saved to the host system and the *Host Profiles* dialog box closes.

- 7 Download the new configuration to the mobile device.

---

**NOTE** For more information about configuring host profiles, see *Chapter 3: Host Profiles* on page 29.

---

## Enabling Battery Strength and Signal Strength Icons

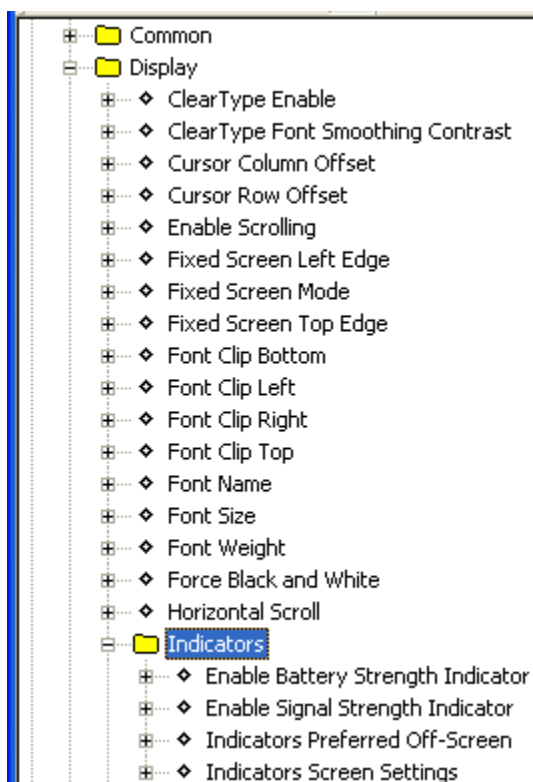
Battery-strength and wireless signal-strength indicator icons are available in Telnet Client 5.1 (and greater versions). You may configure the following indicator-icon settings:

- Whether to display the signal strength icon
- Whether to display the batter power icon

- Whether to display the icon(s) on the Windows system tray, the Telnet Client command bar, or elsewhere on the screen
- The relative size (large or small) of the icon(s)

**To enable the battery power indicator:**

- 1 Access the Configuration Manager for the Telnet Client global emulation parameters.
- 2 In Configuration Manager, locate `Emulation > Display > Indicators`.



**Figure B-16.** *Configuring Indicators*

- 3 Use the `Enable Battery Strength Indicator` parameter to enable/disable the battery strength indicator icon.

- 4 Use the `Enable Signal Strength Indicator` parameter to enable/disable the wireless signal strength indicator.
- 5 Use the `Indicators Preferred Off-Screen` parameter to configure where the icon(s) are displayed (the Windows system tray, the Telnet Client command bar, or on the screen itself).
- 6 If you did not use the `Indicators Preferred Off-Screen` parameter to display icons only in the Windows system tray or Telnet Client command bar, then use the `Indicators Screen Settings` parameter to configure the location and relative size (large or small) of the indicator icon(s) on the screen.
- 7 Save the new configuration.
- 8 Close the Configuration Manager.
- 9 Download the new configuration to the mobile device.

---

**NOTE** For more information about configuring global emulation parameters, see *Chapter 4: Emulation Parameters* on page 61.

---

## Configuring Indicator Settings

Table B-5 provides information about configuring the indicator settings to meet your needs:

Desired Effect	Parameter in Configuration Manager	Setting	Notes
Display icon(s) in Windows task-tray only	Emulation > Display > Indicators > Indicators Preferred Off-Screen	<System Tray Only>	Do not hide the Windows start menu
Display icon(s) in Telnet Client command bar only	Emulation > Display > Indicators > Indicators Preferred Off-Screen	<Command Bar Only>	Do not hide the Telnet Client command bar
Display icon(s) in Telnet Client command bar or Windows system tray (whichever is available, starting with the Windows system tray)	Emulation > Display > Indicators > Indicators Preferred Off-Screen	<Command Bar or System Tray>	—

**Table B-5:** *Configuring Battery and Signal Strength Indicators*

Desired Effect	Parameter in Configuration Manager	Setting	Notes
Display icon(s) on emulation screen (not in the command bar or the system tray)	Emulation > Display > Indicators > Indicators Preferred Off-Screen	<No>	—
Specify location and size of icons	Emulation > Display > Indicators > Indicators Screen Settings	Select your preferred option for location and size	Set Indicators Preferred Off-Screen to No

**Table B-5:** *Configuring Battery and Signal Strength Indicators*

## Appendix C: Using the Telnet Client License Server

This section provides the following information:

- Telnet Client License Server Overview
- Installing the Telnet Client License Server
- Using the License Server

### Telnet Client License Server Overview

The Telnet Client license server is a Windows-based application that provides licenses to mobile devices that are using the Telnet Client.

---

**NOTE** The Telnet Client license server should not be confused with the Avalanche license server. They are separate applications.

---

The Telnet Client license server allows you to store licenses for Telnet Clients at a central location. Those licenses are then automatically distributed to mobile devices that request them.

Telnet Client licenses are distributed to mobile devices in the following manner:

- 1 When the Telnet Client application is first activated on a mobile device, the mobile device broadcasts a request for a license.
- 2 The license server responds to the mobile device with a license.
- 3 The mobile device accepts a license and responds to the license server.

Once a Telnet Client obtains a license, it keeps the license until one of the following criteria are met:

- The license expires.
- The Telnet Client discovers that another mobile device is using the same license.

- The user manually deletes the license from the device.

When any of these criteria are met, the Telnet Client discards the license and requests a new license from the license server.

---

**NOTE** You can also configure the Telnet Client to request a license from a license server on a remote network. For more information about configuring the Telnet Client to request a license from a specific license server, see *Configuring License Server IP Address* on page 239.

---

## License Server Versions and Maintenance Licenses

Currently, three versions of license server are available: version 1.0, version 2.0, and version 3.0. Version 1.0 does not support Telnet Client maintenance licenses or 5.0 (or greater) platform licenses.

If you will be using a license server to distribute 5.0 (or greater) platform licenses or maintenance licenses, please contact Wavelink customer service to obtain the latest version of license server.

---

**NOTE** *Appendix D: Wavelink Contact Information* on page 267 contains Wavelink contact information.

---

### To see which version of license server you have:

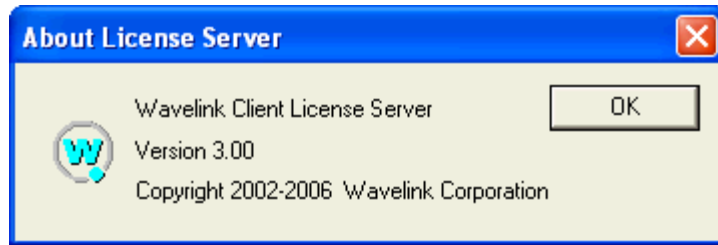
- 1 Launch the license server application.
- 2 Right-click the title bar of the license server window.

A menu list appears.

- 3 Select `About License Server...`

The *About License Server* dialog box appears.





**Figure C-1.** *About License Server Dialog Box*

The *About License Server* dialog box displays the license server version number.

## Installing the Telnet Client License Server

This section provides information about installing the Telnet Client license server as a basic Windows application or as a dedicated Windows service.

### Installation Methods

You may use one of the following methods to install the Telnet Client license server:

- **Windows Application.** When you use this method, the Telnet Client license server runs as a basic application on the host system. If you reboot the host system, you must manually re-launch the license server.
- **Windows Service.** When you use this method, you configure the Telnet Client to run as a dedicated Windows service on the host system. This allows you to automatically restart the license server in the event that the host system must be rebooted. It also allows the license server to operate without requiring a Windows login.

### Installing the License Server as a Windows Application

You can install the Telnet Client as a basic Windows application. In the event that the host system is rebooted, you must manually relaunch the license server application on the host system.

### **Installation Requirements**

Ensure that the system on which you will install the Telnet Client license server meets the following specifications:

- Microsoft Windows 2000/XP or Windows Server
- 2MB hard disk space
- Network connection that provides bi-directional communication with Telnet Clients that will receive licenses from the license server.

### **Installing the License Server**

The Telnet Client license server is a simple executable that should be transferred to the host system.

#### **To install the license server:**

- 1 Obtain the `LicenseServer.exe` file.

---

**NOTE** For information about obtaining client licenses and the Telnet Client license server, contact Wavelink Corporation or your Wavelink representative. *Appendix D: Wavelink Contact Information* on page 267 contains Wavelink contact information.

---

- 2 Copy `LicenseServer.exe` to an accessible location on the host system.

---

**NOTE** You may want to create a shortcut to `LicenseServer.exe` on the desktop of the host system.

---

- 3 Double-click `LicenseServer.exe` to begin running the Telnet Client license server.

The license server interface appears.

---

**NOTE** For information about using the license server, see *Using the License Server* on page 265.

---

## Installing License Server as a Windows Service

It is possible to create a dedicated Windows service from the `LicenseServer.exe` file.

To create a license server service, you will need the Service Installer application that is included in the Microsoft Windows 2000 Resource Kit.

Because creating the license server service requires you to modify Windows registry settings, the exact process that is required is not detailed in this document. Please work directly with Microsoft to configure the license server to run as a dedicated Windows service.

## Using the License Server

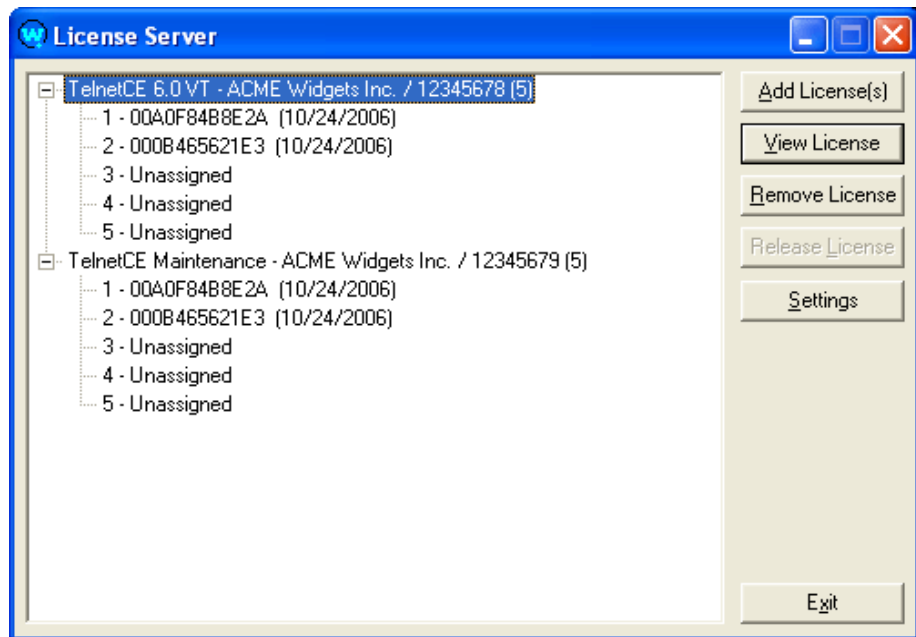
This section provides information about using the Telnet Client license server, including:

- Launching the License Server
- Adding a License
- Releasing a License
- Viewing License Information
- Removing a License

### Launching the License Server

To launch the license server and access the GUI that will allow you to add, remove, and view licenses, execute `LicenseServer.exe`.

When you launch `LicenseServer.exe`, the License Server GUI appears.



**Figure C-2.** License Server GUI

Licenses are displayed in a tree view. Each license type can be expanded to show whether a license is assigned or unassigned. Unassigned licenses will display as **Unassigned**, while assigned licenses will display the MAC address of the mobile device. The date to the right of each license indicates the last time the license connected with the server.

The following is a list of notes about running the license server.

- Only one instance of a license server may be running on the network. If you launch the license server and another license server is running, you will receive an error message.
- If you are running the license server as a Windows service, stop the service before you launch `LicenseServer.exe`.

### **Adding a License**

Add a license to the license server that the license server can then distribute to mobile devices running the Telnet Client.

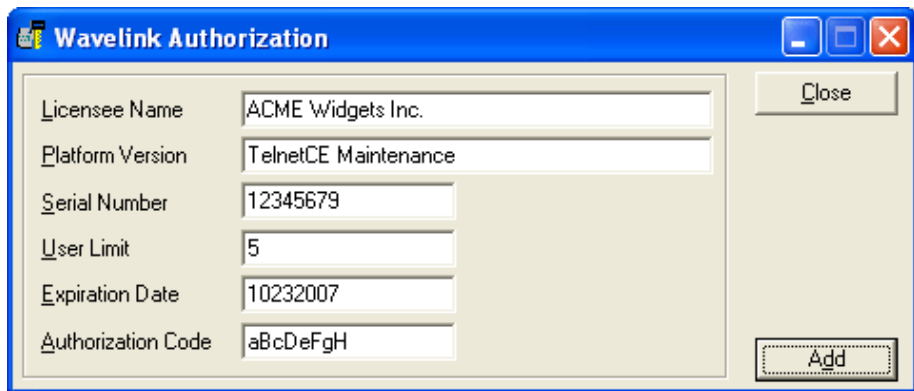
**To add a license to license server:**

- 1 Launch the license server.

The license server GUI appears.

- 2 Click `Add Licenses`.

The *Wavelink Authorization* dialog box appears.



Licensee Name	ACME Widgets Inc.
Platform Version	TelnetCE Maintenance
Serial Number	12345679
User Limit	5
Expiration Date	10232007
Authorization Code	aBcDeFgH

**Figure C-3.** *Wavelink Authorization Dialog Box*

- 3 In the *Wavelink Authorization* dialog box, input the information for the license, where:

- **Licensee Name** is the name of the party to which the license was distributed.
- **Platform Version** is the list of emulation types that the license supports. (The platform version is case sensitive.)
- **Serial Number** is the serial number of the license.
- **User Limit** is the number of users that the license supports.
- **Expiration Date** is the expiration date of the license in the format MMDDYYYY.
- **Authorization Code** is the authorization code for the license.

- 4 After you have input the license information, click `Add`.

A dialog box appears that indicates that the license was successfully added as shown.

- 5 Click `OK`.
- 6 Click `Close` to exit the *Wavelink Authorization* dialog box.

The license now appears in the license server GUI.

- 7 Expand the license to view how many of the user spaces in the license have been taken.

Licenses that have been taken display the MAC address of the mobile device that acquired the license.

## Releasing a License

You can use the license server GUI to free up a license. This does not immediately force the client that holds the license to release that license. Instead, it frees the license for the license server to distribute to another mobile device. You should make sure that the mobile device that previously acquired the license is not operating on the network.

### To release a license:

- 1 Access the license server GUI.
- 2 Locate the license that you want to release.
- 3 Click `Release License`.

The *License Server* dialog box appears.

- 4 Click `Yes`.

The license server GUI now indicates that the client license is unassigned and can be distributed to another mobile device.

## Viewing License Information

You can use the license server GUI to view information about a license.

### To view information about a license:

- 1 Access the license server GUI.

- 2 From the list of installed licenses, select the license that you want to view.

- 3 Click `View License`.

The *View License* dialog box appears and displays the details of the license.

- 4 Click `Close` to close the *View License* dialog box.

## Removing a License

If a license is no longer valid, you may remove it from license server.

### To remove a license from license server:

- 1 Access the license server GUI.

- 2 From the list of licenses that are installed, select the license that you want to remove.

- 3 Click `Remove License`.

The *License Server* dialog box appears and requests confirmation of the deletion.

- 4 Click `Yes`.

The license is deleted from the license server and removed from the license server GUI.

## Changing License Server Settings

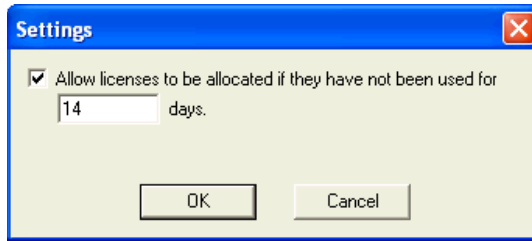
Use the License Server GUI to determine the number of days an unused license can be assigned to a mobile device before it becomes available for redistribution.

### To change settings:

- 1 Launch the License Server GUI.

- 2 Click `Settings`.

The *Settings* dialog box appears.



**Figure C-4.** *Settings Dialog Box*

- 3 Enable the checkbox and enter the number of days (any value between 5 and 365) in the available text box

-Or-

Disable the checkbox to turn this feature off.

---

**NOTE** The default setting is 14 days.

---

- 4 Click **OK**.

The new settings are applied.



---

## **Appendix D: 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](mailto:customerservice@wavelink.com)

**Phone:** 425-823-0111



# Glossary

<b>802.11/a/b</b>	The IEEE standards for wireless Ethernet. 802.11 provides for wireless networking speeds up to 2 Mbps at 2.4 GHz. 802.11b provides wireless networking speeds up to 11 Mbps at 2.4 GHz. 802.11a provides wireless networking speeds up to 54 Mbps at 5 GHz.
<b>access point</b>	A device that acts as a bridge between wireless LANs and wired LANs.
<b>ad hoc mode</b>	A mode of operation in wireless networks wherein wireless devices communicate directly with each other without the use of an access point. Also sometimes referred to as peer-to-peer mode or an independent basic service set (IBSS).
<b>Agent</b>	In the context of Avalanche Manager, an Avalanche Agent. See <i>Avalanche Agent</i> .
<b>AP</b>	Access Point. See <i>Access Point</i> .
<b>automatic WEP</b>	A dynamic implementation of WEP keys, wherein the key used on the wireless network changes periodically. Clients must synchronize their WEP key use with the AP.
<b>Avalanche Agent</b>	An Avalanche Manager Agent. A software component that provides the core functionality of Avalanche Manager. The Agent facilitates communication with Avalanche clients.
<b>Avalanche Client</b>	A mobile device with an installed Avalanche Enabler, which allows the client to communicate with an Avalanche Agent and to be configured and managed through Avalanche Manager.
<b>Avalanche Enabler</b>	A software component that is installed on mobile devices which allows you to configure and manage the device through Avalanche Manager. The Enabler facilitates communication between the mobile device and an Agent.

---

<b>Avalanche Enabler SDK</b>	A software development kit that allows you to create Avalanche Enablers for Windows CE devices.
<b>Avalanche Management Console</b>	The GUI that allows you to interact with and configure Avalanche Agents.
<b>Avalanche Manager</b>	Wavelink Corporation's management application that allows you to configure and manage mobile devices throughout your network infrastructure.
<b>Avalanche Monitor</b>	A component of certain Avalanche Enablers that communicates with the Avalanche Agent and, at certain times, checks for available updates.
<b>Avalanche Update Utility</b>	A component of certain Avalanche Enablers that provides most of the functionality. You can use the Avalanche Update Utility to configure the network parameters of the mobile device, view the progress of a download, and/or install updates that have been downloaded to the client.
<b>Avalanche Software Package</b>	A specially bundled piece of software, for example a firmware update to a radio card or a commonly used application, that you can download to a client through Avalanche Manager.
<b>Avalanche Update</b>	A download (or modification) that is available to a client through Avalanche Manager. Examples of updates include software packages and network profiles. The deletion of orphaned packages from a client through Avalanche Manager is another type of update.
<b>BOOTP</b>	Bootstrap Protocol. A protocol that allows clients to automatically obtain IP parameters from a BOOTP server.
<b>client</b>	In the context of Avalanche Manager, an Avalanche client. See <i>Avalanche Client</i> . In the context of the TNCE Client, a mobile device that connects via the TNCE Client to a host system.
<b>DHCP</b>	Dynamic Host Configuration Protocol. An IP service that allows DHCP clients to automatically obtain IP parameters from a DHCP server.

---

<b>DNS</b>	Domain Name System. A service that provides host name-to-IP address mapping.
<b>.edf</b>	Enabler Definition File
<b>Emulation Parameters</b>	A feature of the TNCE Client that allows you to pre-configure and install terminal emulation-related functions to a mobile device.
<b>Emulation Parameters, global</b>	Terminal emulation-related functions that apply to all host profiles that are configured on a mobile device.
<b>Emulation Parameters, host specific</b>	Terminal emulation-related functions that apply to only a specific host profile that is configured on a mobile device.
<b>Enabler</b>	In the context of Avalanche Manager, an Avalanche Enabler. See <i>Avalanche Enabler</i> .
<b>Enabler Configuration Utility</b>	A software package that allows you to configure the various Avalanche Windows Enabler settings on a client from the Avalanche Management Console. (Specific to the Windows Enabler.)
<b>Enabler Profile</b>	In the context of the Avalanche Enabler SDK, a set of parameters that a developer specifies that are used by the Avalanche Enabler SDK to produce an Avalanche Enabler. The parameters of the profile are stored in an .edf file.
<b>Enabler SDK</b>	See <i>Avalanche Enabler SDK</i> .
<b>ESS ID</b>	Extended Service Set ID. The identifier of an extended service set for devices that are participating in an infrastructure mode wireless LAN.
<b>FTP</b>	File Transfer Protocol. A TCP-based service that provides connection-oriented file transfers.
<b>FTP Server</b>	A host system that provides FTP services. Users are required to log into the FTP service to gain access to files that can be downloaded from the server.

<b>gateway</b>	A device on a local network through which data to other networks is routed. Also called a router.
<b>GUI</b>	Graphical User Interface
<b>host</b>	A server or workstation that hosts a specific software or network service.
<b>host profile</b>	A service of the Telnet Client that allows you to install pre-configured host information (such as IP address and Telnet service TCP port) on mobile devices.
<b>IBSS</b>	Independent Basic Service Set. See <i>ad hoc mode</i> .
<b>ICMP</b>	Internet Control Messaging Protocol. Part of the TCP/IP protocol suite that provides services for testing IP network connections.
<b>IDA Commands</b>	A special value used to invoke a device action, program action, or emulator action within the Telnet Client Industrial Browser.
<b>infrastructure mode</b>	A wireless network configuration wherein devices communicate with each other through an access point.
<b>IP address</b>	Internet Protocol address. A virtual address that uniquely identifies a network connection.
<b>LAN</b>	Local Area Network
<b>lease</b>	A DHCP lease. The parameters surrounding the IP address a client has obtained from a DHCP server.
<b>localization</b>	A service of the TNCE Client that allows you to configure the TNCE Client to display in a specific language.

---

<b>MAC address</b>	Media Access Controller address. The hard-coded layer-2 address of a network connection which consists of a 12-digit hexadecimal number. The first 6 hexadecimal characters identify the manufacturer. The last 6 hexadecimal numbers are unique for each network device produced by the manufacturer. The MAC address is also sometimes called the hardware address.
<b>Management Console</b>	In the context of Avalanche Manager, the Avalanche Management Console. See <i>Avalanche Management Console</i> .
<b>MB</b>	Megabytes
<b>Mbps</b>	Megabits / second
<b>META tag</b>	Tags that allow web pages to enable specific functionality in the browser.
<b>mobile device</b>	A wireless device or a PC with a wireless network connection.
<b>net mask</b>	See <i>subnet mask</i> .
<b>network profile</b>	A set of pre-configured network parameters (ESS ID, IP address, and so forth) that can be downloaded to a client through Avalanche Manager.
<b>orphaned package</b>	A software package that has been deployed to a client through Avalanche Manager, but has been disabled or is not recognized by the Agent. You must orphan a software package before you can use Avalanche Manager to delete it from the client.
<b>ping</b>	An IP service that is used to test IP connectivity. Part of the ICMP service.
<b>RAM</b>	Random Access Memory. Volatile memory in a computer system.

<b>real-time statistics</b>	A feature that allows the Telnet Client to send Telnet session information to Avalanche Manager. That information can then be viewed from the <i>Avalanche Client Controls</i> dialog box. The real-time statistics feature is only available for Avalanche-deployed Telnet Clients.
<b>RF</b>	Radio Frequency. Usually used in the context of a type of network connection.
<b>Resource Editor</b>	A Telnet feature that allows you to import sound and picture files and deploy them to your mobile devices.
<b>router</b>	See <i>gateway</i> .
<b>SDK</b>	Software Development Kit.
<b>selection criteria</b>	A feature of Avalanche Manager that allows you to configure a set of filters that target specific mobile devices on the network. You can filter by MAC address, IP address, device type, operating system, and so forth. Selection criteria are used to target specific mobile devices on the network for Avalanche Updates.
<b>Session Monitor</b>	An Avalanche-integrated component of the Telnet Client that allows a user at the Avalanche Management Console to monitor or control the Telnet Client. Session Monitor is available for Avalanche-deployed Telnet Clients only.
<b>silent install</b>	A feature of the Avalanche Enabler that allows for the installation of software packages on clients without the consent of the user at the client.
<b>silent mode</b>	A feature of the Avalanche Enabler that allows the Avalanche Monitor to run in the background on the client in a manner that is transparent to the user at the client.
<b>software package</b>	In the context of Avalanche Manager, an Avalanche software package. See <i>Avalanche Software Package</i> .



---

<b>SSID</b>	Service Set Identifier. A unique name, up to 32 characters long, that is used to identify a wireless LAN. The SSID is attached to wireless packets and acts as a password to connect to a specific BSS or ESS.
<b>static WEP</b>	Static (or manual) implementation of WEP keys. When the administrator of the network changes the WEP key, users must manually select the correct key.
<b>subnet</b>	A logical network wherein each client is participating on the same IP network.
<b>subnet mask</b>	A type of filter that allows IP clients to determine which part of their IP address defines the network and which part defines the host.
<b>TCP/IP</b>	Transmission Control Protocol/Internet Protocol. A suite of protocols that provides virtual addressing, connection-oriented and connectionless communication, and a number of other network services and utilities.
<b>Telnet</b>	A TCP/IP utility that is used for terminal emulation and that allows a client to connect and interact with a remote host system.
<b>TFTP</b>	Trivial File Transfer Protocol. A UDP-based service that provides connectionless file transfers.
<b>Telnet Client</b>	Wavelink Corporation application that provides client-side terminal emulation services for Microsoft Windows CE-based mobile devices.
<b>update</b>	In the context of Avalanche Manager, an Avalanche update. See <i>Avalanche Update</i> .
<b>WEP</b>	Wired Equivalent Privacy. An encryption standard for wireless networks that provides the equivalent security of a wired connection for wireless transmissions.
<b>Windows CE</b>	A Microsoft Windows-based operating system for mobile devices.

<b>Windows Enabler</b>	An Avalanche Enabler that is designed for Microsoft Windows 9x/ME/NT/2000/XP systems with installed 802.11b wireless cards.
<b>WINS</b>	Windows Internet Naming Service. A service that provides Windows name-to-IP address mapping.

# Index

## Numerics

- 5250/3270 virtual keyboard 143
- 802.11/a/b 273

## A

- about
  - emulation parameters 63
  - global emulation parameters 64
  - host profiles 12
  - keyboard creator 13
  - localization 12
  - maintenance licenses 123
  - per-host emulation parameters 63
  - platform licenses 123
  - scripting 12
  - SSL 12
  - Telnet Client 10
- access point 273
- accessing
  - global emulation parameters 64
  - per-host emulation parameters 69
- activation method 83
  - on barcode, MSR or RFID Scan 86
  - on key combination 84
  - on screen update 87
  - select from menu 84
  - when session connects 85
- activetext
  - configuring 250
  - using 149
- ad hoc mode 273
- adding
  - a license 266
  - host profiles 34
- agent 273
- alphabetized view, configuration manager 76
- AP 273

- authorization 121
- autologin for VT emulation, configuring 253
- automatic WEP 273
- Avalanche Agent 273
- Avalanche client 273
- Avalanche Enabler 273
- Avalanche Enabler SDK
  - edf, defined 275
  - enabler profile, defined 275
- Avalanche Management Console, defined 274
- Avalanche Manager, defined 274
- Avalanche Monitor, defined 274
- Avalanche software package, defined 274
- Avalanche update 274
- Avalanche update utility, defined 274

## B

- battery strength icon 257
- beeps settings 220
- BOOTP 274

## C

- certificate verification, enabling 41
- client 274
- cold boot recovery 18
- COM port, freeing 229
- concurrent telnet sessions, configuring 241
- configuration manager
  - alphabetized view 76
  - find 75
  - using 72
- configuration support matrix 20
- configuring
  - activetext 250
  - autologin for VT emulation 253
  - emulation parameters 64
  - failover 46

- host profiles 33
- IP printing 242
- key macros 247
- license server IP address 243
- number of concurrent sessions 241
- passwords 239
- scan handlers 251
- screen panning 248
- session monitor 186
- Telnet Client 18
- Telnet Client display settings 244
- Telnet Client lockdown 245
- Telnet Client with Avalanche Manager 21
- Telnet Client with Microsoft ActiveSync 23
- telnet negotiation strings for VT emulation 254
- TermProxy-only connections 44
- workstation IDs for 5250/3270 emulation 256
- connecting to hosts 129
- contact information 271
- creating script code 88
- cursor settings 218
- D**
  - deleting host profiles 36
  - demo license, using 127
  - deploying
    - configurations 24
    - configurations via Avalanche Manager 24
    - configurations via Microsoft ActiveSync 30
    - Resource Editor files 119
  - deploying keyboards 113
  - deploying scripts 100
  - developing
    - web pages 167
  - DHCP 274
  - diagnostics utility
    - accessing 151
    - performing a keyboard test 152
    - performing a scan test 154
    - performing a Windows keyboard test 155
  - diagnostics utility, using 151
  - disconnecting a Telnet session 135
  - display settings 215
  - display settings, configuring 244
  - DNS 275
  - document
    - assumptions 9
    - conventions 9
- E**
  - edit autologin 204
  - editing scripts 96
  - emulation parameters
    - about 12, 63
    - configuring 64
    - defined 275
    - global 64
    - global, defined 275
    - manually configuring 205
    - modifying 74
    - per-host 63
    - per-host, defined 275
    - using configuration manager 72
  - Emulation Parameters, global 275
  - Emulation Parameters, host specific 275
  - Enabler 275
  - Enabler configuration utility 275
  - Enabler profile 275
  - enabling
    - certificate verification 41
    - indicator icons 257
    - session monitor 186
    - SSL 39
  - ESSID 275
  - executing scripts
    - on barcode, MSR or RFID scan 102
    - on key combination 101

- on screen update 102
- select from menu 100
- when session connects 101

exiting the Telnet Client 136

exporting 98

exporting scripts 98

## **F**

Field Data ID 96

find 75

font settings 213

freeing a COM port 229

FTP 275

FTP server 275

## **G**

gateway 276

global emulation parameters

- about 64
- accessing 64

GUI 276

## **H**

host 276

host failover 46

host profile, defined 276

host profiles 90

- about 12
- adding 34
- and SSL 38
- and TermProxy 44
- configuration settings 60
- configuring 33
- deleting 36
- edit autologin 204
- host settings 48
- IBM settings 53
- manually configuring 197
- modifying 35
- more 5250 options 202

- more VT options 203
- overview 31
- TermProxy settings 51
- VT settings 55
- WEB settings 53

## **I**

IBM Host settings 208

IBSS 276

ICMP 276

IDA Commands 175

IDA Commands,defined 276

importing keyboard graphics 109

importing scripts 97

indicator icons 257

Industrial Browser

- basic navigation 166
- host profile settings 166
- overview 159
- using 166

infrastructure mode 276

initiating a Telnet session 133

installing

- license server 263
- SSL support package on host system 38
- SSL support package on mobile device 39
- Telnet Client 17

IP address 276

IP printing, configuring 242

## **K**

key macros, configuring 247

keyboard creator

- about 13
- launching 103
- overview 103

keyboard files 105

keyboard test 152

keyboards

- adding 106

- creating 106
- deleting 108
- deploying 113
- importing graphics 109
- keys 109
- positioning rows 112
- sizing 108
- sizing rows 112
- keys
  - adding keys 110
  - configuring 109
  - creating 109
  - deleting 113
  - positioning 112
  - sizing 112

**L**

- LAN 276
- launching
  - Resource Editor 115
  - session monitor 188
  - Telnet Client 129
  - Telnet Client from Avalanche 131
  - Telnet Client from Windows 130
- lease 276
- license server
  - installation methods 263
  - installing 263
  - using 265
  - versions 262
- license server IP address, configuring 243
- licenses
  - maintenance 123
  - platform 123
- licensing
  - adding a license 266
  - demo license 127
  - manually licensing the Telnet Client 124
  - methods 122, 123
  - overview 121

- releasing a license 268
- removing a license 269
- the Telnet Client 121
- types 123
- using license server 125
- viewing license information 268
- localization
  - about 12
  - defined 276
- lockdown, configuring 245

## **M**

- MAC address 277
- maintenance licenses
  - about 123
  - license server versions 262
- management console 277
- MB 277
- Mbps 277
- message settings 209
- META tag, defined 277
- META tags 167
- Microsoft ActiveSync
  - creating a guest partnership 234
  - creating a standard partnership 230
  - freeing a COM port 229
  - selecting connection method on host system 226
  - selecting mobile device connection method 225
- mobile device 277
- modifying
  - emulation parameters 74
  - host profiles 35
  - real-time statistics 195
- more 5250 options 202
- more VT options 203
- multiple concurrent sessions 137

**N**

- net mask 277

network profile, defined 277

## O

options menu 156  
orphan package, defined 277  
orphaned package 277

## P

partnership  
    creating a standard partnership 230  
    guest partnership 234  
passwords, configuring 239  
performing script capturing 92  
per-host emulation parameters  
    about 63  
    accessing 69  
    beeps settings 220  
    cursor settings 218  
    display settings 215  
    font settings 213  
    IBM host settings 208  
    Industrial Browser settings 209  
    manually configuring 207  
    message settings 209  
    printer settings 221  
    telnet settings 220  
    view settings 216  
    VTXX settings 207  
ping 277  
platform license 123  
printer settings 221

## R

RAM 277  
real-time statistics 191  
    modifying 195  
    viewing 192  
releasing a license 268  
removing a license 269  
Resource Editor

    adding bitmap 116  
    adding sound 117  
    deploying files 119  
    editing files 117  
    launching 115  
    overview 115  
    playing sounds 117  
    using 116  
RF 278  
router 278

## S

saving scripts 98  
scan handlers, configuring 251  
scan test 154  
screen panning  
    configuring 248  
    using 149  
script capturing 92  
script code 88  
script editor 79  
    launching from Avalanche Manager 80  
scripting  
    about 12  
    creating variables 88  
scripts 98  
    activation method 83  
    creating scripts 82  
    deploying 100  
    editing 96  
    Field Data ID 96  
    importing 97  
    overview 79  
    saving 98  
SDK 278  
selecting  
    host profiles 90  
    Microsoft ActiveSync connection on host  
        system 226

- Microsoft ActiveSync connection on mobile device 225
  - selection criteria 278
  - session monitor
    - configuring 186
    - enabling 186
    - launching 188
    - session override 189
    - tracing sessions 190
    - using 186
  - signal strength icon 257
  - silent install 278
  - silent mode 278
  - sizing keyboards 108
  - software packages, defined 278
  - SSID 279
  - SSL
    - about 12
    - and host profiles 38
    - enabling 39
    - enabling certificate verification 41
    - installing support package on host system 38
    - installing support package on mobile device 39
  - standard partnership, creating 230
  - static WEP 279
  - subnet 279
  - subnet mask 279
  - switching between active Telnet sessions 139
- T**
- tables
    - Telnet Client version and supported features matrix 14
    - text-formatting conventions 10
  - TCP/IP 279
  - telnet 279
  - Telnet Client 279
    - about 10
    - authorizing 121
    - autologin for VT emulation 253
    - cold boot recovery 18
    - components 11
    - configuration support matrix 20
    - configuring 18
      - configuring activetext 250
      - configuring display settings 244
      - configuring IP printing 242
      - configuring key macros 247
      - configuring license server IP address 243
      - configuring lockdown 245
      - configuring number of concurrent sessions 241
      - configuring passwords 239
      - configuring scan handlers 251
      - configuring screen panning 248
      - configuring telnet negotiation strings for VT emulation 254
      - configuring with Avalanche Manager 21
      - configuring with Microsoft ActiveSync 23
      - configuring workstation id 256
    - deployment methods 11
    - diagnostics utility 151
    - disconnecting a session 135
    - exiting 136
    - functionality 13
    - initiating a Telnet session 133
    - installing 17
    - launching 129
    - licensing 121
      - licensing with license server 125
    - manually configuring emulation parameters 205
    - manually configuring host profiles 197
    - manually licensing 124
    - multiple concurrent sessions 137
    - options menu 156
    - overview 10
    - real-time statistics 191
    - session monitor 186



- using 129
- version and supported features matrix 14
- telnet negotiation strings, configuring 254
- telnet settings 220
- TermProxy
  - and host profiles 44
  - configuring failover 46
  - configuring TermProxy-only connections 44
- TFTP 279
- tracing sessions 190

## U

- updates, defined 279
- using
  - activetext 149
  - configuration manager 72
  - find 75
  - Industrial Browser 166
  - license server 265
  - real-time statistics 191
  - Resource Editor 116
  - screen panning 149
  - session monitor 186
  - session override 189
  - standard virtual emulation keyboard 141
  - Telnet Client 129
  - Telnet Client diagnostics utility 151
  - Telnet Client options menu 156

## V

- variables 88
- version and supported features matrix 14
- view settings 216
- viewing license information 268
- viewing real-time statistics 192
- virtual keyboard
  - 5250/3270 143
  - using 141
  - VT/HP 145

- WEB 145
- VT/HP virtual keyboard 145
- VTXX settings 207

## W

- Wavelink contact information 271
- web pages
  - developing 167
  - IDA Commands 175
  - META tags 167
  - printing 169
  - scanner 171
  - specifying the home page 166
  - symbologies 173
- WEB settings
  - Access List 159
  - HTTP Proxy 159
  - HTTPS Proxy 159
- WEB virtual keyboard 145
- WEP
  - automatic 273
  - defined 279
  - static wep 279
- Windows CE 279
- Windows Enabler 280
- WINS 280
- workstation id, configuring 256

