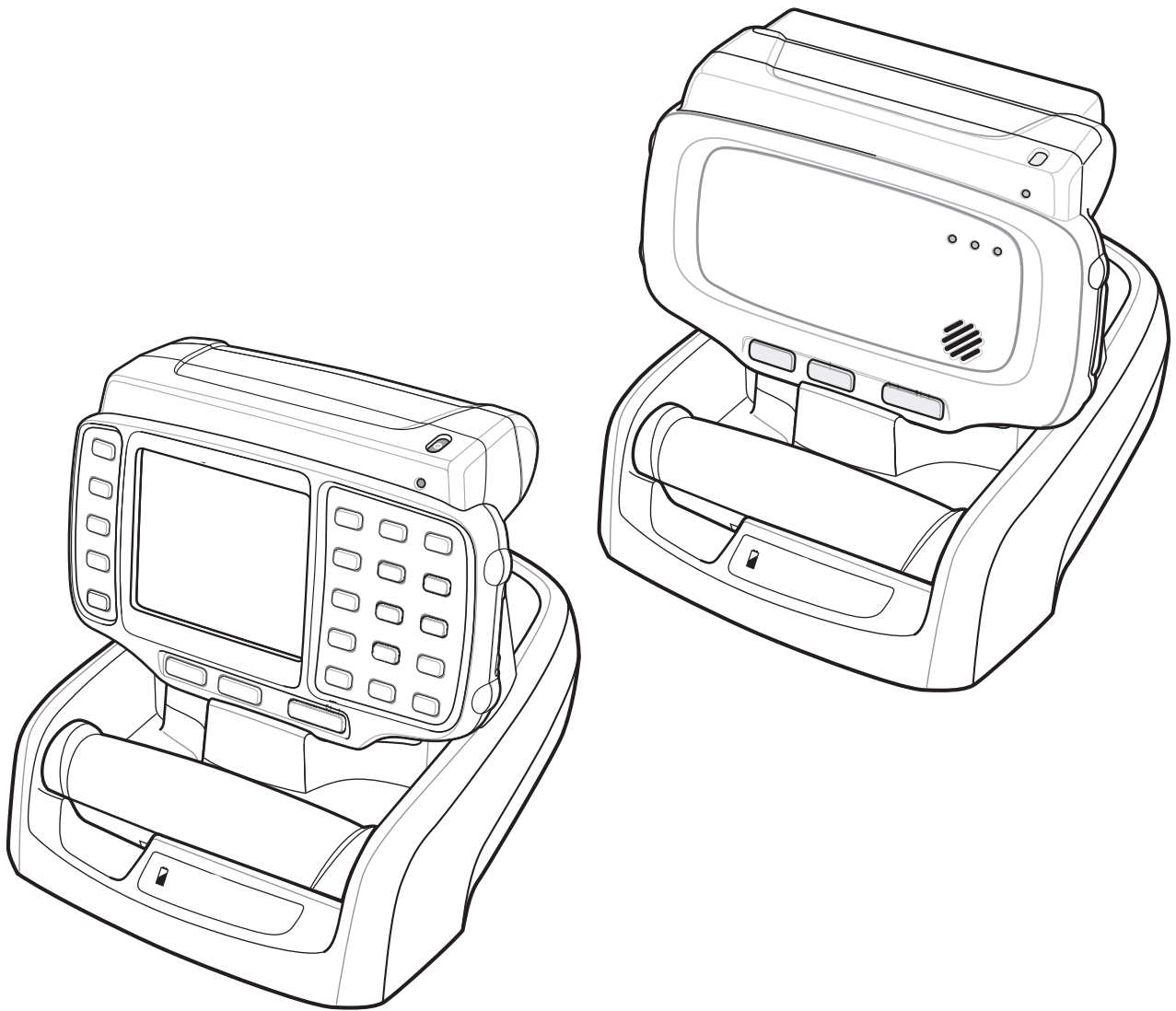


WT4070/90 Wearable Terminal

Integrator Guide



***WT4070/90 Wearable Terminal
Integrator Guide***

72E-87638-07

Rev. A

April 2015

© 2015 ZIH Corp

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 Zebra. 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. Zebra 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 Zebra. 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 Zebra. The user agrees to maintain Zebra’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.

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

Zebra does not assume any product liability arising out of, or in connection with, the application or use of any product, circuit, or application described herein.

No license is granted, either expressly or by implication, estoppel, or otherwise under any Zebra, intellectual property rights. An implied license only exists for equipment, circuits, and subsystems contained in Zebra products.

Revision History

Changes to the original manual are listed below:

Change	Date	Description
-01 Rev. A	9/29/06	Initial release.
-02 Rev. A	03/28/07	Add 128 MB configuration, wall mounting bracket, Fusion 2.5 information.
-03 Rev. A	05/06/08	Add BTEplorer support and freezer pouch information.
-04 Rev. A	12/20/08	Add touch screen configuration.
-05 Rev. A	03/03/09	Update Ethernet cradle daisy chaining information.
-06 Rev. A	12/15/09	Add Voice Only WT4090 information.
-07 Rev. A	04/30/15	Zebra re-branding.

Table of Contents

Revision History	iii
------------------------	-----

About This Guide

Introduction	xiii
Documentation Set	xiii
Configurations	xiv
Software Versions	xiv
Chapter Descriptions	xv
Notational Conventions	xvi
Related Documents and Software	xvi
Service Information	xvii

Chapter 1: Getting Started

Introduction	1-1
Unpacking the Wearable Terminal	1-1
Getting Started	1-4
Installing and Removing the Main Battery	1-4
Installing the Main Battery	1-4
Charging the Battery	1-5
Charging the Main Battery and Memory Backup Battery	1-5
Charging Spare Batteries	1-6
Removing the Main Battery	1-6
Starting the Wearable Terminal	1-7
WT4070/90 Boot Up	1-7
Voice Only WT4090 Boot Up	1-7
Checking Battery Status	1-7
Configuring the Wearable Terminal	1-8
Resetting the Wearable Terminal	1-8
Performing a Warm Boot	1-8
Performing a Cold Boot	1-8
Battery Management	1-8
Battery Saving Tips	1-8
Changing the Power Settings	1-9

Changing the Display Backlight Settings	1-9
Changing the Keypad Backlight Settings	1-9
Turning the WLAN Radios Off	1-10
Long Term Storage	1-10

Chapter 2: Accessories

Introduction	2-1
Cradles	2-1
Charger	2-1
Miscellaneous	2-1
Single Slot USB Cradle	2-2
Battery Charging Indicators	2-4
Communication Setup	2-5
Four Slot Ethernet Cradle	2-6
Daisy chaining Cradles	2-7
Ethernet Cradle Drivers	2-8
Charging and Communication	2-9
Battery Charging Indicators	2-10
Speed LED	2-10
Link LED	2-10
Four Slot Spare Battery Charger	2-11
Spare Battery Charging	2-11
Battery Charging Indicators	2-12
Wall Mount Bracket	2-13
Power Supply Installation	2-14
Four Slot Ethernet Cradle Installation	2-15
Four Slot Battery Charger Installation	2-17
Wiring	2-17
Placing a Battery in the Charger	2-19
Mounting Multiple Brackets	2-19
Navigating the Wearable Terminal with an External Input Device	2-21
USB Device	2-21
Bluetooth Mouse	2-23
Connector Shroud	2-24
Assembly	2-24
Disconnecting the Cable from the Wearable Terminal	2-24

Chapter 3: ActiveSync

Introduction	3-1
Installing ActiveSync	3-1
Wearable Terminal Setup	3-2
Setting Up an ActiveSync Connection on the Host Computer	3-2
Setting up a Partnership	3-3

Chapter 4: Voice Only WT4090 Remote Control

Introduction	4-1
MotoRC Software	4-1

Microsoft ActiveSync Remote Display Software	4-1
Connection to Host Computer	4-1
MotoRC Connection	4-2
Microsoft ActiveSync Remote Display Connection	4-3

Chapter 5: Wireless Applications

Introduction	5-1
Signal Strength Icon	5-2
Turning the WLAN Radio On and Off	5-3
Find WLANs Application	5-3
Profile Editor Wizard	5-4
Profile ID	5-4
Operating Mode	5-5
Ad-Hoc	5-7
Authentication	5-7
Tunneled Authentication	5-8
User Certificate Selection	5-10
User Certificate Installation	5-10
Server Certificate Selection	5-11
Credential Cache Options	5-12
User Name	5-14
Password	5-14
Advanced Identity	5-15
Encryption	5-15
Key Entry Page	5-17
Passkey Dialog	5-17
IP Address Entry	5-18
Transmit Power	5-20
Battery Usage	5-21
Manage Profiles Application	5-22
Changing Profiles	5-23
Editing a Profile	5-23
Creating a New Profile	5-24
Deleting a Profile	5-24
Ordering Profiles	5-24
Export a Profile	5-24
Wireless Status Application	5-25
Signal Strength Window	5-25
Current Profile Window	5-27
IPv4 Status Window	5-27
Wireless Log Window	5-29
Saving a Log	5-29
Clearing the Log	5-29
Versions Window	5-29
Wireless Diagnostics Application	5-30
ICMP Ping Window	5-31
Trace Route Window	5-31
Known APs Window	5-32
Options	5-33

Operating Mode Filtering	5-33
Regulatory Options	5-34
Band Selection	5-35
System Options	5-35
Change Password	5-36
Export	5-37
Persistence	5-38
Registry Settings	5-38
Log On/Off Application	5-39
User Already Logged In	5-39
No User Logged In	5-39

Chapter 6: Using Bluetooth

Introduction	6-1
Adaptive Frequency Hopping	6-1
Security	6-2
Turning the Bluetooth Radio Mode On and Off	6-3
Disabling Bluetooth	6-3
Enabling Bluetooth	6-3
Bluetooth Power States	6-4
Cold Boot	6-4
Warm Boot	6-4
Suspend	6-4
Resume	6-4
Bluetooth Profiles	6-4
Accessing BTE Explorer	6-6
Using App Launcher	6-6
Using Key Combination	6-6
BTE Explorer Navigation	6-6
Key Combinations	6-6
Discovering Bluetooth Device(s)	6-7
Available Services	6-10
File Transfer Services	6-10
Create New File or Folder	6-11
Delete File	6-12
Get File	6-12
Put File	6-13
Connect to Internet Using Access Point	6-13
OBEX Object Push Services	6-14
Headset Services	6-15
Serial Port Services	6-15
Personal Area Network Services	6-16
HID Services	6-16
Bonding with Discovered Device(s)	6-17
Accepting a Bond	6-18
Trusted Devices Window	6-19
Deleting a Bonded Device	6-20
Connecting to a Favorite Service	6-20
Navigating the Favorites Window	6-21

Delete all Favorite Services	6-21
Delete a Favorite Service	6-21
Rename a Favorite Service	6-22
Change the Display View	6-22
View Active Connections	6-22
View Properties	6-22
Bluetooth Settings	6-23
Device Info Tab	6-23
Services Tab	6-23
File Transfer Service	6-24
OBEX Object Push Service	6-25
Personal Area Networking Service	6-25
Serial Port Service	6-26
Headset Service	6-27
Headset Audio Gateway Service Information Service	6-27
Security Tab	6-28
Discovery Tab	6-28
Virtual COM Port Tab	6-29
HID Tab	6-30
Miscellaneous Tab	6-30

Chapter 7: Application Deployment

Software Installation on Development PC	7-1
Device Configuration Package	7-1
Platform SDK	7-2
Enterprise Mobility Developer Kits	7-2
Installing Other Development Software	7-2
Deployment	7-2
OSUpdate	7-3
Update Loader	7-3
ActiveSync	7-3
IPL	7-4
Creating Hex Images	7-5
Starting Terminal Configuration Manager	7-6
Defining Script Properties	7-7
Creating the Script for the Hex Image	7-8
Opening a New or Existing Script	7-9
Updating TCM 1.X Scripts	7-9
Copying Components to the Script	7-9
Saving the Script	7-9
Building the Image	7-9
Sending the Hex Image Using IPL	7-11
WT4070/90	7-11
Voice Only WT4090	7-15
TCM Error Messages	7-16
IPL Error Detection	7-17
Voice Only WT4090 IPL Error Indications	7-19
Creating a Splash Screen	7-19
Flash Storage	7-20

FFS Partitions	7-20
Working with FFS Partitions	7-20
RegMerge.dll	7-21
CopyFiles	7-21
Non-FFS Partitions	7-22
Downloading Partitions to the Wearable Terminal	7-22

Chapter 8: Staging and Provisioning

Introduction	8-1
Rapid Deployment (RD) Client	8-1
AirBEAM Smart Client	8-1
MSP 3 Agent	8-1

Chapter 9: Special Considerations

Touch Panel User Interface Considerations	9-1
Tips for Improving Battery Life	9-1
Display Backlight	9-1
Keypad Light	9-2
Power	9-2
Wireless LAN	9-3
Voice Only WT4090 LED Considerations	9-3

Chapter 10: Maintenance & Troubleshooting

Introduction	10-1
Maintaining the Wearable Terminal	10-1
Wrist Mount Cleaning Instructions	10-2
Arm Sleeve Cleaning Instructions	10-2
Removing the Screen Protector	10-2
Battery Safety Guidelines	10-3
Cleaning	10-4
Materials Required	10-4
Cleaning the Wearable Terminal	10-4
Housing	10-4
Display	10-4
Connectors	10-4
Cleaning the RS309, RS409 and RS507	10-5
Housing	10-5
Scanner Exit Window	10-5
Connectors	10-5
Cleaning Cradle Connectors	10-5
Cleaning Frequency	10-6
Troubleshooting	10-6
Wearable Terminal	10-6
Four Slot Spare Battery Charger	10-10
Four Slot Ethernet Cradle	10-10
Single Slot USB Cradle	10-11

Appendix A: Technical Specifications

- Technical Specifications A-1
 - Wearable Terminal A-1
 - RS309 Scanner A-4
 - RS409 Scanner A-5
 - RS507 Scanner A-7
 - Accessories A-9

Glossary

Index

About This Guide

Introduction

This guide provides information about setting up and configuring WT4070 and WT4090 wearable terminals and accessories. The WT4090 has two versions, one with a display and a voice only version without a display. Throughout this guide Voice Only WT4090 refers to the version without the display and WT4070/90 refer to the version with a display.

✓ **NOTE** Screens and windows pictured in this guide are samples and can differ from actual screens.

Documentation Set

The documentation set for the WT4070/90 is divided into guides that provide information for specific user needs.

- **Microsoft Application Guide** - describes how to use Microsoft developed applications.
- **Application Guide** - describes how to use Zebra developed applications.
- **WT4070/90 Wearable Terminal User Guide** - describes how to use the WT4070/90 wearable terminal.
- **WT4070/90 Wearable Terminal Integrator Guide** - describes how to set up the WT4070/90 wearable terminal and the accessories.
- **EMDK Help File** - provides API information for writing applications.

Configurations

This guide covers the following configurations:

Configuration	Radios	Display	Memory	Data Capture	Operating System	Keypads
WT4070	WLAN: 802.11b/g WPAN: Bluetooth	2.8" QVGA Color non-touch	128 MB RAM/ 64 MB Flash	Optional accessory	Windows CE 5.0 Professional	Two-color or Triple-tap Alphanumeric Keypad
WT4090	WLAN: 802.11a/b/g WPAN: Bluetooth	2.8" QVGA Color non-touch	128 MB RAM/ 64 MB Flash or 128 MB RAM/ 128 MB Flash	Optional accessory	Windows CE 5.0 Professional	Two-color or Triple-tap Alphanumeric Keypad
		2.8" QVGA Color; touch	128 MB RAM/ 128 MB Flash	Optional accessory	Windows CE 5.0 Professional	Two-color Alphanumeric Keypad
Voice Only WT4090	WLAN: 802.11a/b/g WPAN: Bluetooth	None	128 MB RAM/ 128 MB Flash	Optional accessory	Windows CE 5.0 Professional	Three key

Software Versions

- ✓ **NOTE** To view the software versions on the Voice Only WT4090, the Voice Only WT4090 must be connected to a host computer running remote desktop software. See [Chapter 4, Voice Only WT4090 Remote Control](#) for more information.

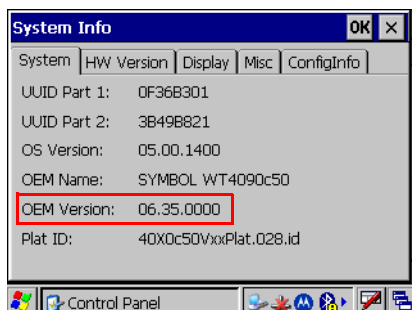
This guide covers various software configurations and references are made to operating system or software versions for:

- OEM version
- Fusion version.

OEM Software

To determine the OEM software version:

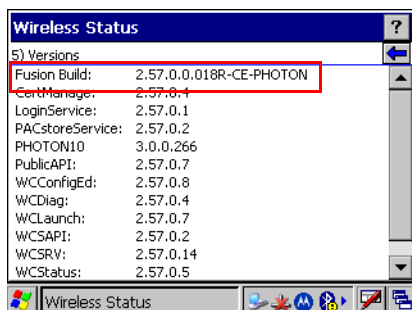
1. Press **CTRL** and then **ESC** to open the **Start** menu.
2. Using the navigation keys, select Settings.
3. Press the Blue key and the down arrow to open the **Control Panel** sub-menu.
4. Press **ENTER** key to launch **Control Panel**.
5. Using the navigation keys, select the **System Information** icon.
6. Press **ENTER** key to launch **System Information** applet.



Fusion Software

To determine the Fusion software version:

1. Press **ALT - w**. The **Wireless** menu appears.
2. Using the navigation keys, select **Wireless Status**.
3. Press **ENTER**. The **Wireless Status** window displays.
4. Press **5**. The Versions screen appears.



Chapter Descriptions

Topics covered in this guide are as follows:

- [Chapter 1, Getting Started](#), lists the accessories for the wearable terminal and explains how to install and charge the batteries and start the wearable terminal for the first time.
- [Chapter 2, Accessories](#), describes the accessories available for the wearable terminal.
- [Chapter 3, ActiveSync](#), provides instructions on installing ActiveSync and setting up a partnership between the wearable terminal and a host computer.
- [Chapter 5, Wireless Applications](#), provides instructions on using and configuring the wearable terminal on a wireless network.
- [Chapter 6, Using Bluetooth](#), explains Bluetooth functionality on the wearable terminal.
- [Chapter 7, Application Deployment](#), provides instructions for installing the Device Configuration Package (DCP) for WT40x0 and the SMDK for C on the host computer and downloading software and files to the wearable terminal.
- [Chapter 10, Maintenance & Troubleshooting](#), includes instructions on cleaning and storing the wearable terminal, and provides troubleshooting solutions for potential problems during wearable terminal operation.

- [Appendix A, Technical Specifications](#), includes a table listing the technical specifications for the wearable terminal and accessories.

Notational Conventions

The following conventions are used in this document:

- “Wearable terminal” refers to the Zebra WT4070/90 series of wearable terminals.
- *Italics* are used to highlight the following:
 - Chapters and sections in this guide
 - Related documents
- **Bold** text is used to highlight the following:
 - Dialog box, window and screen names
 - Drop-down list and list box names
 - Check box and radio button names
 - Icons on a screen
 - Key names on a keypad
 - Button names on a screen.
- Bullets (•) indicate:
 - Action items
 - Lists of alternatives
 - Lists of required steps that are not necessarily sequential.
- Sequential lists (e.g., those that describe step-by-step procedures) appear as numbered lists.

Related Documents and Software

The following documents provide more information about the WT4090 wearable terminals.

- *WT4070/90 Quick Start Guide*, p/n 72-86717-xx
- *Voice Only WT4090 Quick Start Guide*, p/n 72-130435-xx
- *WT4070/90 Windows® CE 5.0 Regulatory Guide*, p/n 72-86718-xx
- *WT4070/90 Wearable Terminal User Guide*, p/n 72E-87633-xx
- *RS309 Scanner Quick Reference Guide*, p/n 72-86011-xx
- *RS409 Scanner Quick Reference Guide*, p/n 72-86010-xx
- *RS507 Hands-free Imager Quick Reference Guide*, p/n 72-115987-xx
- *RS507 Hands-free Imager Product Reference Guide*, p/n 72E-120802-xx
- *Application Guide for Zebra Devices*, p/n 72E-68901-xx
- *Wireless Fusion Enterprise Mobility Suite User Guide for Version X.XX*
- *Microsoft Applications for Windows Mobile and CE 5.0 User Guide*, p/n 72E-78456-xx

- *Enterprise Mobility Developer Kits*, available at: <http://www.zebra.com/support>.
- Device Configuration Package (DCP for WT4090c50) and Platform SDK (PSDK9090c50) for WT4090 with Windows CE 5.0, available at: <http://www.zebra.com/support>.
- Latest ActiveSync software, available at: <http://www.microsoft.com>.

For the latest version of this guide and all guides, go to: <http://www.zebra.com/support>.

Service Information

If you have a problem with your equipment, contact Zebra support for your region. Contact information is available at: <http://www.zebra.com/support>.

When contacting support, please have the following information available:

- Serial number of the unit
- Model number or product name
- Software type and version number

Zebra responds to calls by e-mail, telephone or fax within the time limits set forth in support agreements.

If your problem cannot be solved by Zebra Support, you may need to return your equipment for servicing and will be given specific directions. Zebra is not responsible for any damages incurred during shipment if the approved shipping container is not used. Shipping the units improperly can possibly void the warranty.

If you purchased your business product from a Zebra business partner, contact that business partner for support.

Chapter 1 Getting Started

Introduction

This chapter lists the accessories for the wearable terminal and explains how to install and charge the batteries and start the wearable terminal for the first time.

Unpacking the Wearable Terminal

Carefully remove all protective material from around the wearable terminal and save the shipping container for later storage and shipping.

Verify that you received all equipment listed below:

- Wearable terminal
- Lithium-ion battery
- Regulatory Guide
- Quick Start Guide (poster).

Inspect the equipment for damage. If you are missing any equipment or if you find any damaged equipment, contact Zebra Support immediately. See [Service Information on page xvii](#) for contact information.

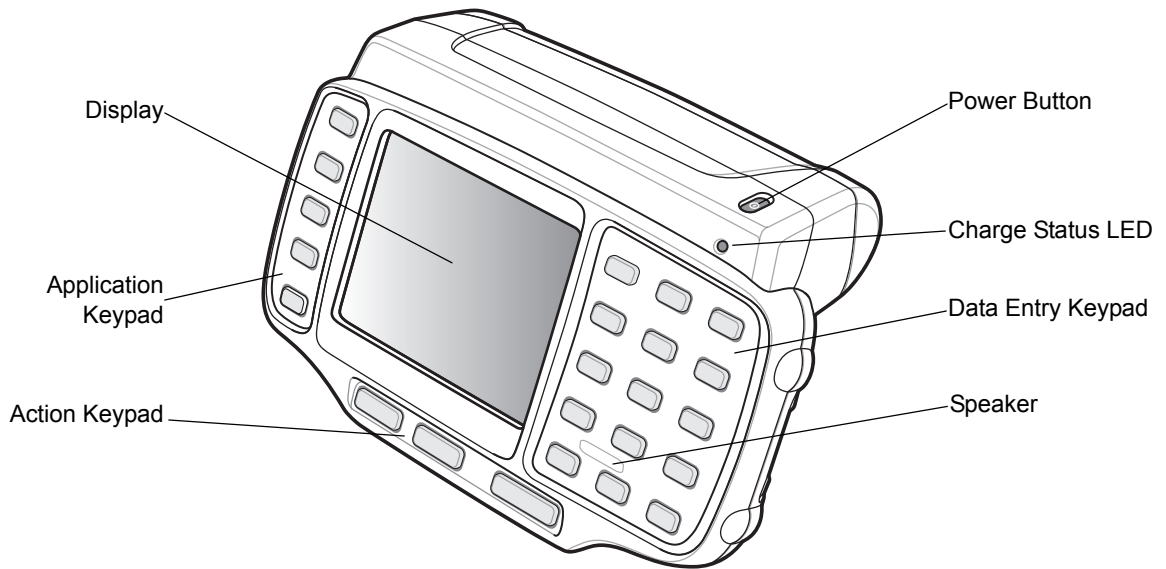


Figure 1-1 WT4070/90 Wearable Terminal Front View

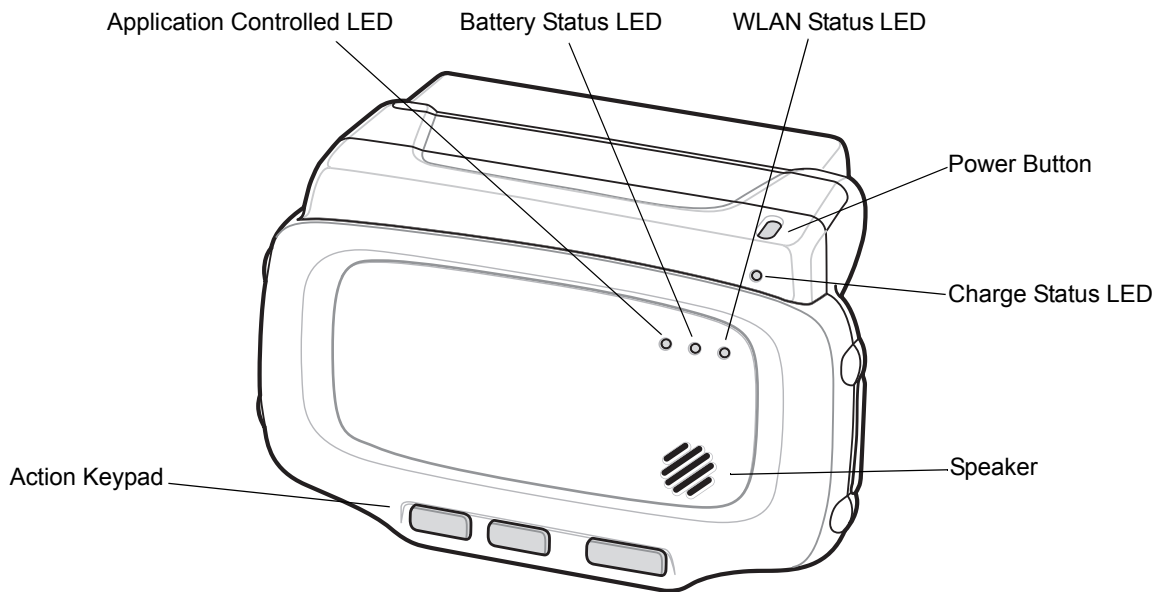


Figure 1-2 Voice Only WT4090 Wearable Terminal Front View

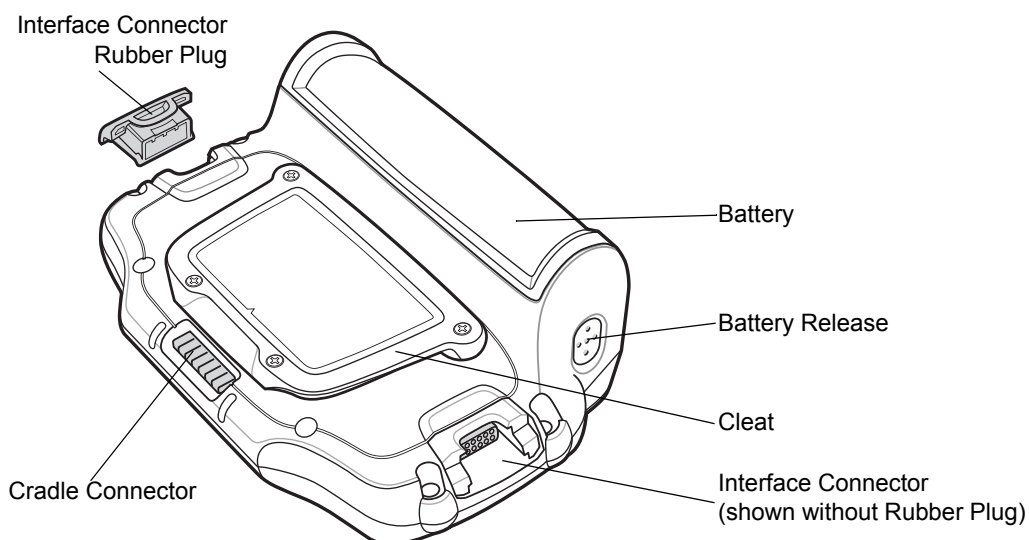


Figure 1-3 *Wearable Terminal Back View*

Table 1-1 *Parts of the Wearable Terminal*

Item	Description
Display	Displays the application and data stored on the device. (WT470/090 only)
Power Button	Places the wearable terminal in to the suspend mode or resumes normal operation. Performs a warm boot when held down for five seconds. See <i>Resetting the Wearable Terminal</i> on page 2-17 for information about performing a warm boot.
Charge Status LED	By default, indicates the charging status of the battery.
WLAN Status LED	By default, indicates the status of the wireless connection. (Voice Only WT4090 only)
Battery Indicator LED	By default, indicates when the battery charge level falls below 30%. (Voice Only WT4090 only)
Application LED	Application programmable. (Voice Only WT4090 only)
Speaker	Provides audio playback.
Keypads	Enable user input.
Battery	Provides power to the wearable terminal.
Interface Connector	Provides electrical connection to an accessory, such as a scanner.
Cradle Connector	Provides electrical connection to a cradle.
Battery Release	Releases the battery for removal.
Cleat	Provides mounting for the wrist mount and cradles.

Getting Started

In order to start using the wearable terminal for the first time:

- Install the main battery
- Charge the main battery and backup battery
- Start the wearable terminal.

✓ **NOTE** The main battery can be charged before or after installation into the wearable terminal. Use the Single Slot USB cradle or Four Slot Spare Battery Charger to charge the main battery before installation, or the Single Slot USB cradle or Four Slot Ethernet cradle to charge the main battery after installation.

Installing and Removing the Main Battery

Installing the Main Battery

Before using the wearable terminal, install a lithium-ion battery by placing the battery into the wearable terminal as shown in [Figure 1-4](#).

✓ **NOTE** Ensure the battery is fully inserted. An audible click can be heard as the battery is fully inserted. A partially inserted battery may result in unintentional data loss.

When a battery is fully inserted in a wearable terminal for the first time, upon the wearable terminal's first power up, the device boots and powers on automatically.

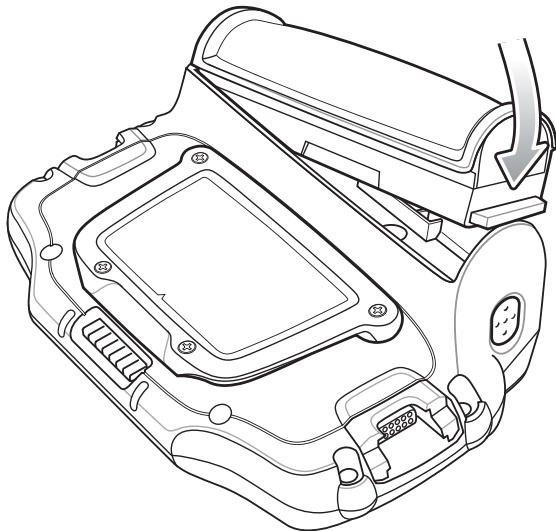


Figure 1-4 *Installing the Main Battery*

Charging the Battery



CAUTION Ensure that you follow the guidelines for battery safety described in [Battery Safety Guidelines on page 10-3](#).

Charging the Main Battery and Memory Backup Battery

Before using the wearable terminal for the first time, charge the main battery until the amber Charge Status LED remains lit (see [Table 1-2 on page 1-5](#) for charge status indications).

The wearable terminal is equipped with a memory backup battery which automatically charges from the main battery whether or not the wearable terminal is operating or is in suspend mode. The memory backup battery retains data in memory for at least 30 minutes when the wearable terminal's main battery is removed or fully discharged. When the wearable terminal is used for the first time or after the memory backup battery has fully discharged, the memory backup battery requires approximately 15 hours to fully charge. Do not remove the main battery from the wearable terminal for 15 hours to ensure that the memory backup battery fully charges. If the main battery is removed from the wearable terminal or the main battery is fully discharged, the memory backup battery completely discharges in several hours.

When the wearable terminal reaches a very low battery state, the combination of main battery and backup battery retains data in memory for at least 24 hours.



NOTE Do not remove the main battery within the first 15 hours of use. If the main battery is removed before the backup battery is fully charged, data may be lost.

Charge the wearable terminal with an installed main battery using either the Single Slot USB cradle or the Four Slot Ethernet cradle.

To charge the main battery:

1. Ensure the cradle used to charge the main battery is connected to the appropriate power source.
2. Insert the wearable terminal into a cradle.
3. The wearable terminal starts to charge automatically. The amber Charge Status LED lights to indicate the charge status. See [Table 1-2](#) for charging indications.

Table 1-2 *Wearable Terminal LED Charge Indicators*

LED	Indication
Off	Wearable terminal is not in cradle. Wearable terminal not placed correctly. Charger is not powered.
Fast Blinking Amber	Charging error: <ul style="list-style-type: none"> • Temperature is too low or too high. • Charging has gone on too long without completing (typically eight hours).
Slow Blinking Amber	Wearable terminal is charging.
Solid Amber	Charging complete. Note: When the battery is initially inserted in the wearable terminal, the amber LED flashes once if the battery power is low or the battery is not fully inserted.

Charging Spare Batteries

Use the following accessories to charge spare batteries:

- Single Slot USB cradle
- Four Slot Spare Battery charger.

To charge a spare battery:

1. Ensure the accessory used to charge the spare battery is connected to the appropriate power source.
2. Insert the spare battery into the accessory's spare battery charging slot with the charging contacts facing down (over the charging pins) and gently press down on the battery to ensure proper contact.
3. The battery starts to charge automatically. The amber charge LED on the accessory lights to show the charge status. See [Chapter 2, Accessories](#) for accessory charge LED indicator definitions.

Removing the Main Battery

To remove the main battery:

1. Prior to removing the battery, ensure that the wearable terminal is in suspend mode. If the wearable terminal is not in suspend mode, press the Power button to place the wearable terminal in suspend mode.
2. Press the battery release button. The battery partially ejects from the wearable terminal.
3. Remove the battery from the wearable terminal.

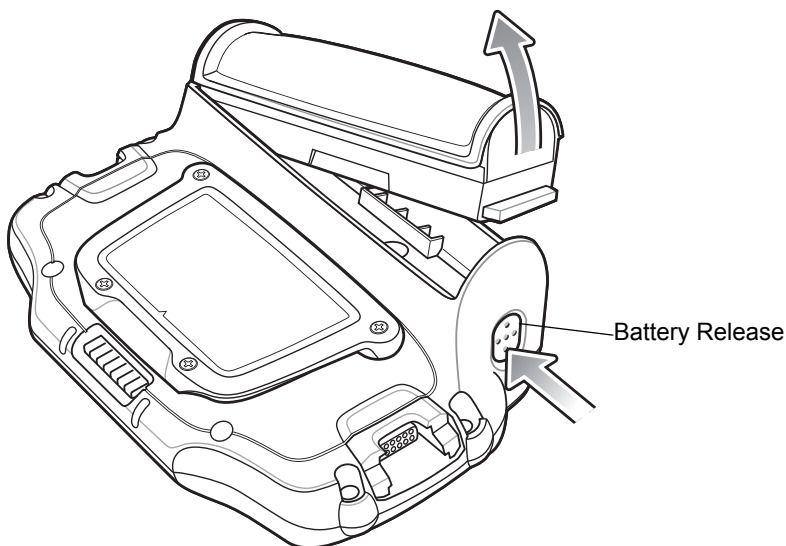


Figure 1-5 Removing the Main Battery

Starting the Wearable Terminal

Press the **Power** button to turn on the wearable terminal. If the wearable terminal does not power on, perform a cold boot. See [Performing a Cold Boot on page 1-8](#).

✓ **NOTE** When a battery is fully inserted in a wearable terminal for the first time, upon the wearable terminal's first power up, the device boots and powers on automatically.

WT4070/90 Boot Up

When the WT4070/90 is powered on for the first time the splash screen appears for a short period of time followed by the Start Up window on non-touch configurations and the calibration screen on touch enabled configurations.



Figure 1-6 Start Up Window App Launcher

Voice Only WT4090 Boot Up

When the Voice Only WT4090 is powered on for the first time the three LEDs on the front housing blink as follows:

Application Controlled LED and Battery Status LED on.

All LEDs off.

Application Controlled LED on, Battery Status LED on, WLAN Status LED on.

WLAN Status LED off, Battery Status LED off, Application Controlled LED off.

The WLAN Status LED blinks indicating that the wireless connection is not connected or is solid indicating that the wireless connection is connected.

Checking Battery Status

✓ **NOTE** To navigate using the keypad refer to the *WT4070/90 Wearable Terminal User Guide*.

To check whether the main battery or backup battery in the wearable terminal is charged:

1. Select **Start > Settings > Control Panel > Power** icon to display the **Battery Status** window.
2. Press **ENTER**.

To save battery power, set the wearable terminal to turn off after a specified number of minutes.

Configuring the Wearable Terminal

- To customize the wearable terminal settings, refer to the *Microsoft Applications for Mobile and CE 5.0 User Guide*.
- To set up ActiveSync to synchronize the wearable terminal with the host computer, see [Chapter 3, ActiveSync](#).
- To configure the wearable terminal for wireless LAN network, see [Chapter 5, Wireless Applications](#).
- To deploy software on the wearable terminal, see [Chapter 7, Application Deployment](#).

Resetting the Wearable Terminal

There are two reset functions, warm boot and cold boot. A warm boot restarts the wearable terminal by closing all running programs.

A cold boot also restarts the wearable terminal, but erases all stored records and entries in RAM. Data saved in flash memory is not lost. In addition it returns formats, preferences and other settings to the factory default settings.

Perform a warm boot first. This restarts the wearable terminal and saves all *stored* records and entries. If the wearable terminal still does not respond, perform a cold boot.

Performing a Warm Boot

Hold down the Power button for approximately five seconds. As soon as the wearable terminal starts to perform a warm boot release the Power button.

Performing a Cold Boot

A cold boot restarts the wearable terminal and erases all user stored records and entries that are not saved in flash memory (Application and Platform folders). *Never perform a cold boot unless a warm boot does not solve the problem.*

✓ **NOTE** Any data previously synchronized with a computer can be restored during the next ActiveSync operation.

To perform a cold boot on a WT4070/90 press and simultaneously hold the Power button and the **1** and **9** keys. Do not hold down any other keys or buttons. The wearable terminal initializes.

To perform a cold boot on a Voice Only WT4090 press and simultaneously hold the **P1** and **P2 keys**, and the Power button. The Voice Only WT4090 initializes.

Battery Management

Battery Saving Tips

- Place the wearable terminal in a cradle connected to AC power at all times when not in use.

- Set the wearable terminal to turn off after a short period of non-use.
- Set the display and keypad backlight to turn off after a short period of non-use.
- Turn on the keypad backlight only if needed.
- Turn off all wireless radio activity when not in use.

Changing the Power Settings

✓ **NOTE** To navigate using the keypad refer to the *WT4070/90 Wearable Terminal User Guide*.

To set the wearable terminal to turn off after a short period of non-use:

1. Select **Start > Settings > Control Panel > Power icon > Power Off** tab.
2. Press **ENTER**.
3. Select the **On battery power: Turn off device if not used for:** check box and select a value from the drop-down list box.
4. Press **ENTER**.

Changing the Display Backlight Settings

✓ **NOTE** To navigate using the keypad refer to the *WT4070/90 Wearable Terminal User Guide*.
Not applicable on the Voice Only WT4090.

Changing the Backlight setting on the Voice Only WT4090 will change the brightness of the Application Controlled LED. Refer to the EMDK Help file WT4090-VOW Programming page for more information.

To change the display backlight settings in order to conserve more battery power:

1. Select **Start > Settings > Control Panel > Backlight icon > Battery Power** tab.
2. Press **ENTER**.
3. Select the **On battery power: Disable backlight if not used for:** check box and select a value from the drop-down list box.
4. Select the **Brightness** tab.
5. Select the **Disable backlight** check box to completely turn off the display backlight.
6. Use the slider to set the brightness of the backlight. Set it to a low value to save battery power.
7. Press **ENTER**.

Changing the Keypad Backlight Settings

✓ **NOTE** To navigate using the keypad refer to the *WT4070/90 Wearable Terminal User Guide*.
Not applicable on the Voice Only WT4090.

Changing the Keypad Backlight setting on the Voice Only WT4090 will change the brightness of the WLAN Status LED. Refer to the EMDK Help file WT4090-VOW Programming page for more information.

To change the keypad backlight settings in order to conserve more battery power:

1. Select **Start > Settings > Control Panel > Keylight icon > Battery Power** tab.
2. Press **ENTER**.
3. Select the **On battery power: Disable keylight if not used for:** check box and select a value from the drop-down list box.
4. Select the **Advanced** tab.
5. Select the **Disable keylight** check box to completely turn off the keypad backlight.
6. Press **ENTER**.

Turning the WLAN Radios Off

✓ **NOTE** To navigate using the keypad refer to the *WT4070/90 Wearable Terminal User Guide*.

To turn off the WLAN radio:

1. Press **ALT - w**. The Wireless menu appears.
2. Select **Disable Radio**.
3. Press **ENTER**.

To turn on the radio:

1. Press **ALT - w**. The Wireless menu appears.
2. Select **Enable Radio**.
3. Press **ENTER**.

Long Term Storage

When storing the wearable terminal for a long period of time it is recommended to place the wearable terminal in storage mode.

1. Remove the main battery.
2. On the WT4070/90, press and simultaneously hold the **1, 9** keys and Power button (cold boot).

or

On the Voice Only WT4090, press and simultaneously hold the **P1** and **P2** keys and the Power button (cold boot).

3. Release the keys and Power button.

When returning the wearable terminal to everyday operation, install a fully charged main battery.

Chapter 2 Accessories

Introduction

Wearable terminal accessories provide a wide variety of product support capabilities. Accessories include cradles, a battery charger, scanners and headsets. For all accessories not covered in this chapter, refer to the *WT4070/90 Wearable Terminal User Guide*.

Cradles

- Single Slot USB cradle charges the wearable terminal main battery and a spare battery. It also synchronizes the wearable terminal with a host computer through a USB connection.
- Four Slot Ethernet cradle charges up to four wearable terminal main batteries and up to four spare batteries. It also provides the wearable terminal with an Ethernet connection.

Charger

- Four Slot Spare Battery Charger charges up to four wearable terminal spare batteries.

Miscellaneous

- Wall mount bracket
- Connector shroud.

Single Slot USB Cradle



CAUTION Ensure that you follow the guidelines for battery safety described in [Battery Safety Guidelines on page 10-3](#).

This section describes how to set up and use a Single Slot USB cradle with the wearable terminal. For USB communication setup procedures see [Communication Setup on page 2-5](#).

The Single Slot USB cradle:

- Provides 5.4 VDC power for operating the wearable terminal.
- Provides USB ports for data communication between the wearable terminal and a host computer or other serial devices (e.g., a printer).



NOTE The normal function of the product may be disturbed by Strong Electro Magnetic Interference (for example, static electricity). If so, simply remove and re-insert the terminal to resume normal operation. In case the function does not resume, please use the product in another location.

- Synchronizes information between the wearable terminal and a host computer. (With customized or third party software, it can also be used to synchronize the wearable terminal with corporate databases.)
- Charges the wearable terminal's battery.
- Charges a spare battery.
- Provides a location for storing an attached scanner during charging.



CAUTION Use only an approved power supply output rated 12 VDC and minimum 3.3 A. Use of an alternative power supply will void the product warranty and may cause product damage. Refer to the *WT4070/90 User Guide* for the power supply regulatory compliance statement.

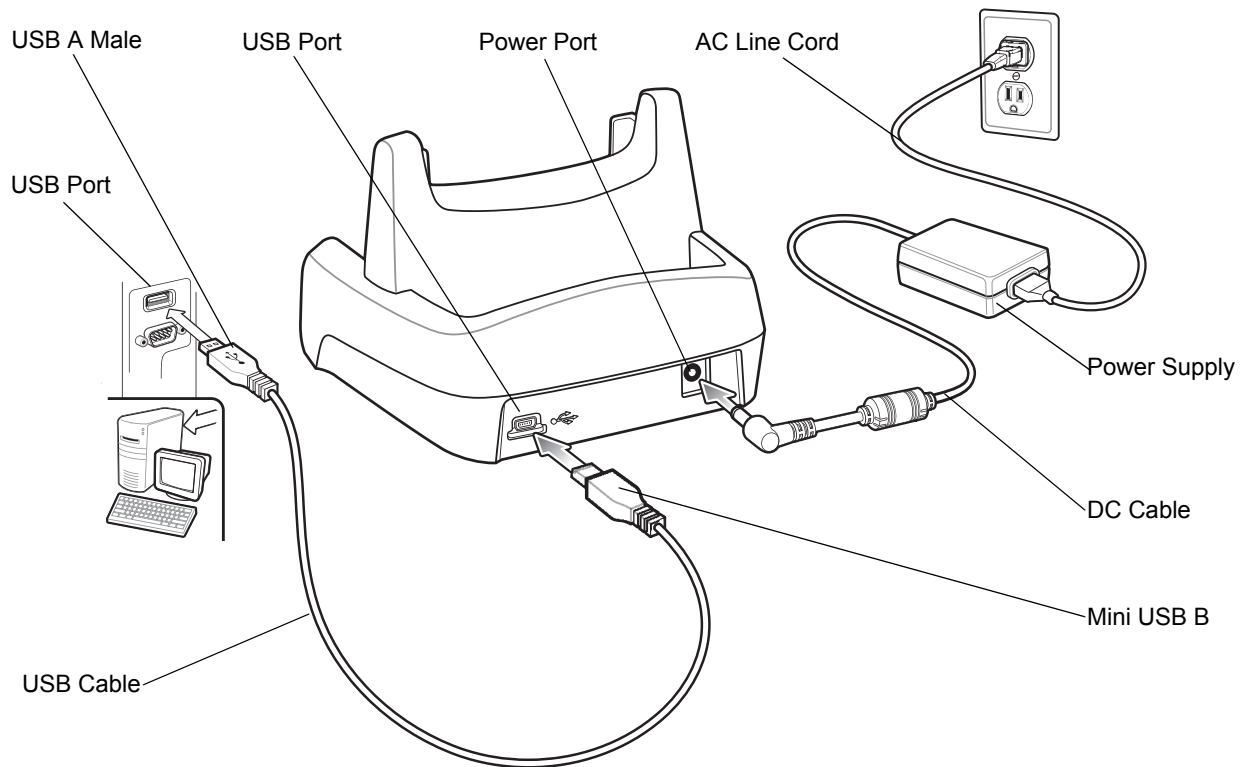


Figure 2-1 *Single Slot USB Cradle Setup*

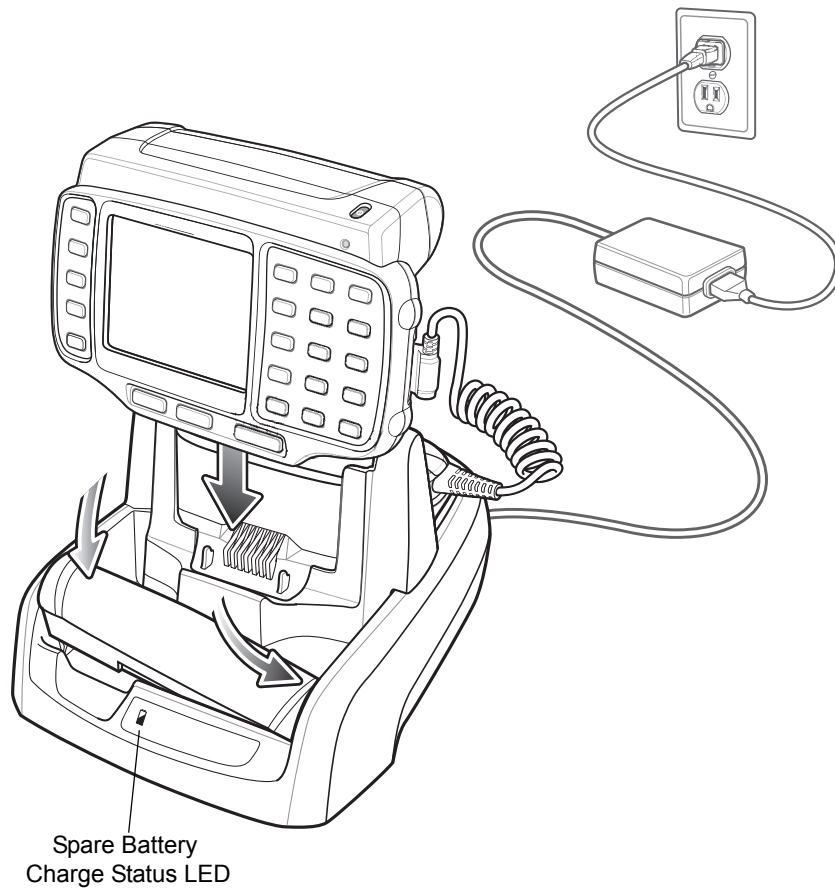


Figure 2-2 Wearable Terminal and Spare Battery Charging

Battery Charging Indicators

The Single Slot USB cradle can charge the wearable terminal's main battery and a spare battery simultaneously. The wearable terminal's amber Charge Status LED indicates the status of the battery charging in the wearable terminal. See [Table 1-2 on page 1-5](#) for charging status indications. The amber Spare Battery Charge Status LED on the cradle (see [Figure 2-1 on page 2-3](#)) indicates the status of the spare battery charging in the cradle. See [Table 2-1](#) for charging status indications. The standard capacity batteries usually charge in less than four hours and the extended capacity battery usually charges in less than eight hours.

Table 2-1 Spare Battery Charge Status LED Indicator

Spare Battery LED (on cradle)	Indication
Off	No spare battery in well; spare battery not placed correctly; cradle is not powered.
Fast Blinking Amber	Charging error: <ul style="list-style-type: none"> • Temperature is too low or too high. • Charging has gone on too long without completing (typically eight hours).
Slow Blinking Amber	Spare battery is charging.
Solid Amber	Charging complete.

Communication Setup

The wearable terminal can communicate with a host computer using the Single Slot USB cradle. By default the wearable terminal is configured to communicate using USB. Ensure that ActiveSync on the host computer is set to allow USB connections.

1. Ensure that ActiveSync was installed on the host computer and a partnership was created.
2. Start ActiveSync if it is not running on the host computer. To start, select **Start > Programs > Microsoft ActiveSync**.

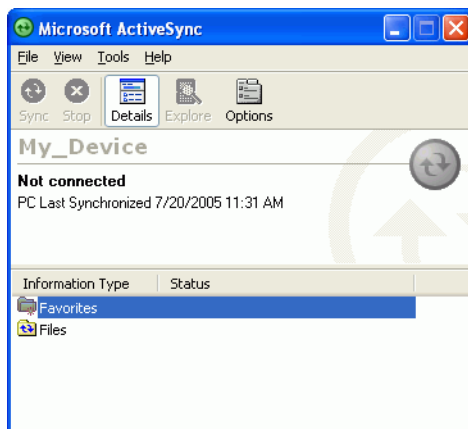


Figure 2-3 ActiveSync - Not Connected

3. In the ActiveSync window, select **File > Connection Settings**. The Connection Settings window displays.



Figure 2-4 Connection Settings

4. Select **Allow USB connection** check box.
5. Select **OK** to save any changes made.
 - ✓ **NOTE** Every wearable terminal should have a unique device name. Never try to synchronize more than one wearable terminal to the same name. The device name is set in the **System Properties** window.
6. Connect the device to the host computer.
 - ✓ **NOTE** The cradle requires a dedicated port. It cannot share a port with an internal modem or other device. Refer to the computer user manual supplied to locate the serial port(s).
7. Upon connection, synchronization occurs automatically.

Four Slot Ethernet Cradle



CAUTION Ensure that you follow the guidelines for battery safety described in [Battery Safety Guidelines on page 10-3](#).

This section describes how to set up and use a Four Slot Ethernet cradle with the wearable terminal.

The Four Slot Ethernet cradle:

- Provides 5.4 VDC power for operating up to four wearable terminals.
- Enables data communication between the wearable terminal (up to four) and a host computer, over an Ethernet network (using a standard 10Base-T Ethernet cable).
- Simultaneously charges up to four wearable terminals (with batteries installed).

You cannot ActiveSync using the Four Slot Ethernet cradle. To ActiveSync with a host computer, use the Single Slot USB cradle.



CAUTION Use only an approved power supply output rated 12 VDC and minimum 9 A. Use of an alternative power supply will void the product warranty and may cause product damage. See the *WT4070/90 User Guide* for the power supply regulatory compliance statement.

Connect the Ethernet cradle (Ethernet port 1) to an Ethernet hub or a port on the host device. Connect the Ethernet cradle (power port) to an approved power supply.

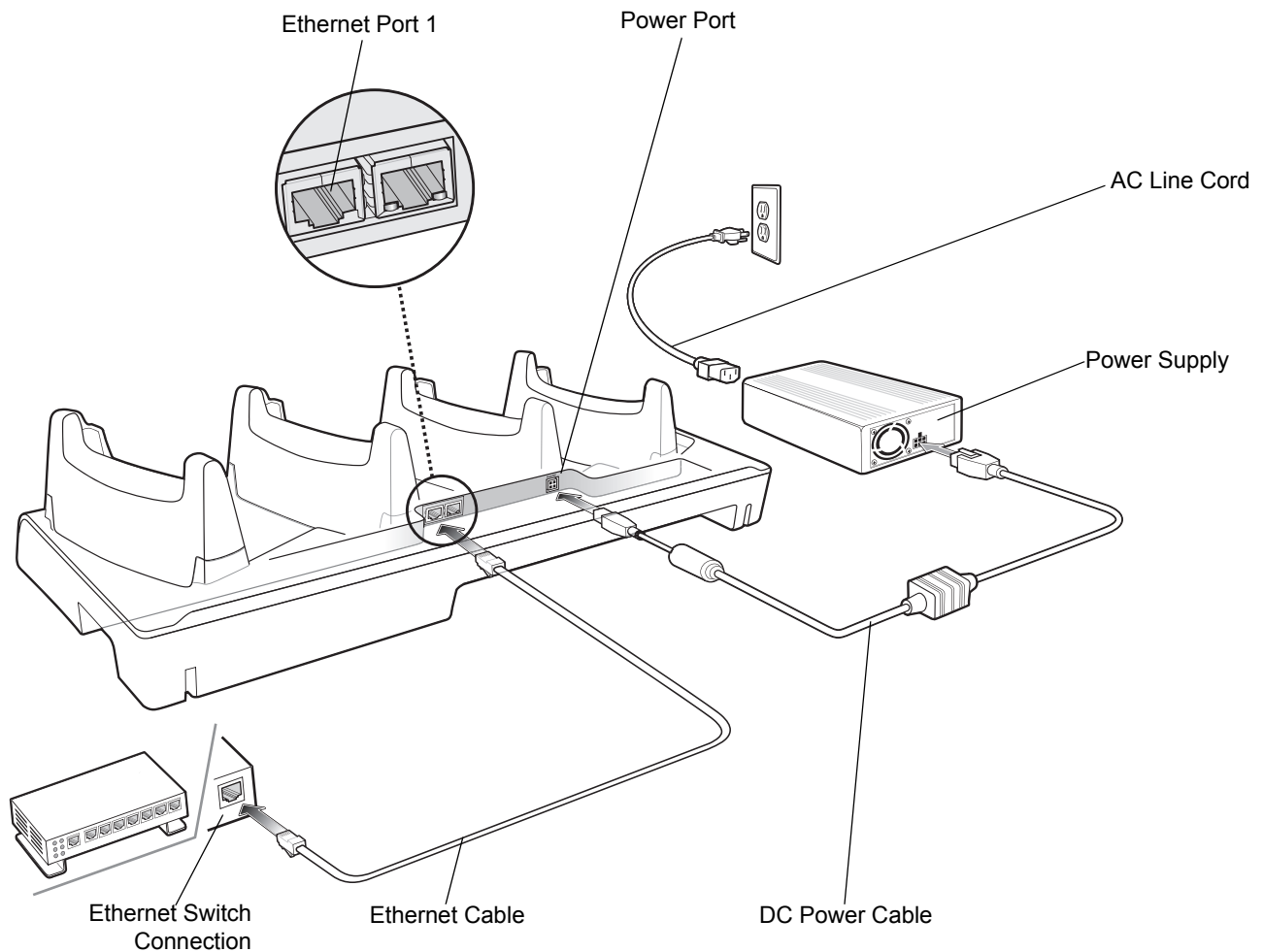


Figure 2-5 Four Slot Ethernet Cradle Setup

Daisy chaining Cradles

To connect several cradles to an Ethernet network, up to four Ethernet cradles may be daisy chained. Daisy-chaining should not be attempted when the main Ethernet connection to the first cradle is 10 Mbps as throughput issues will certainly result. The Speed LED and the Link LED on the Ethernet port 2 function in the same way as the Speed LED and the Link LED on the front of the cradle.

To daisy chain cradles:

1. Connect the first Ethernet cradle to power and to the Ethernet switch as shown on [Figure 2-5 on page 2-7](#).
2. Connect power to the second Ethernet cradle.
3. Connect the daisy chain Ethernet cable (either straight or twisted cable can be used) between Ethernet Port 2 of the first cradle, and Ethernet Port 1 of the second cradle.
4. Connect additional cradles as described in Step 2 and Step 3.

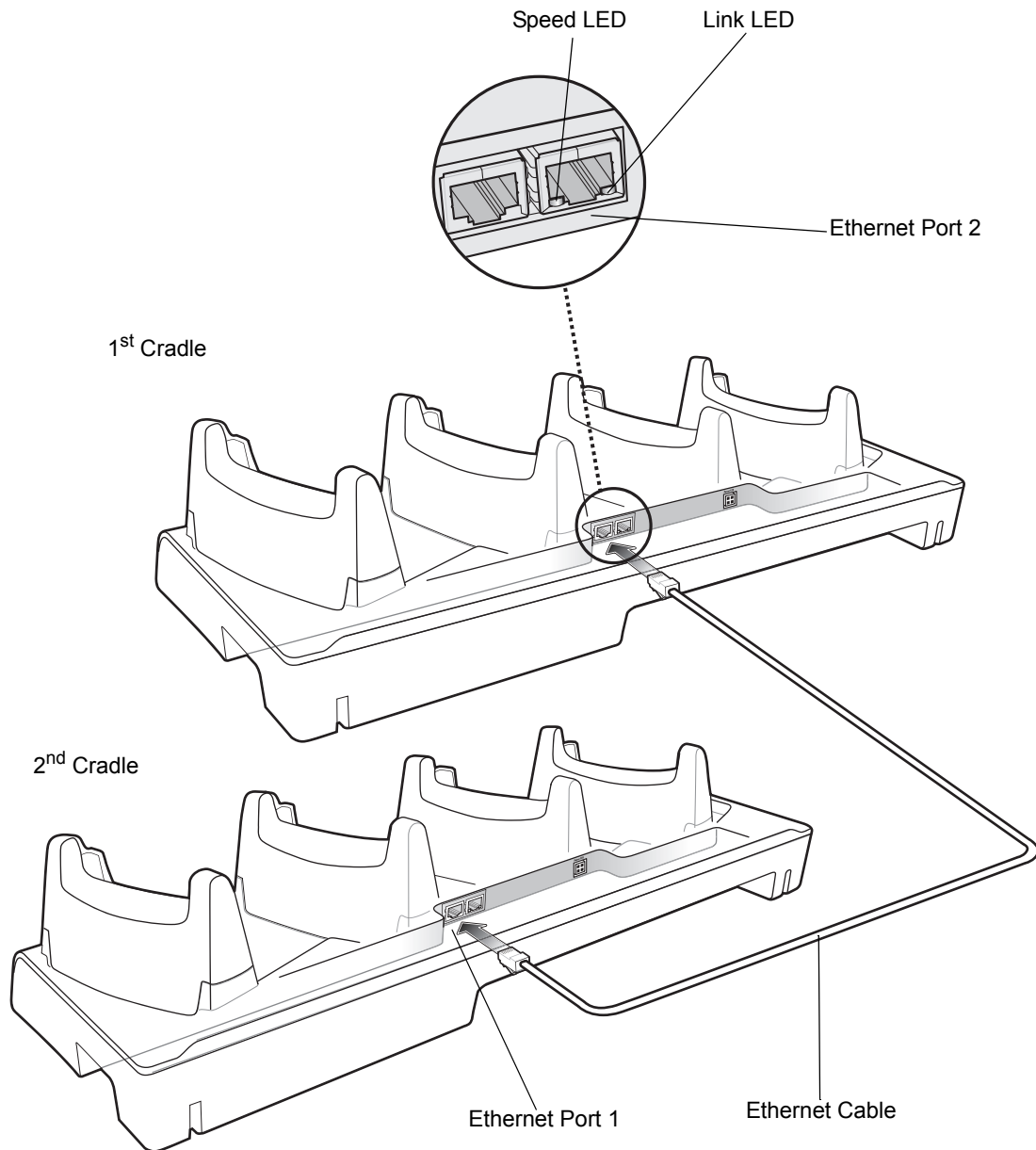


Figure 2-6 *Daisy chaining Four Slot Ethernet Cradles*

Ethernet Cradle Drivers

The Ethernet cradle drivers are pre-installed on the wearable terminal and initiate automatically when the wearable terminal is placed in a properly connected Four Slot Ethernet cradle. When the wearable terminal is inserted into the Four Slot Ethernet cradle, the LAN icon appears in the Windows CE 5.0 desktop taskbar and indicates that the wearable terminal is connected to a network.

✓ **NOTE** The device's IP address can only be viewed on the WT4070/90.

To view the IP Address assigned to the wearable terminal open a **Command Prompt** window and enter `ipconfig`. Press **CTRL > ESC**.

1. Use the navigation keys to select **Programs**.
2. Press **ENTER** to open the sub-menu.
3. Use the navigation keys to select **Command Prompt**.
4. Press **ENTER**. The **Command Prompt** window displays.
5. Enter `ipconfig`. The window displays the IP Address assigned to the wearable terminal.

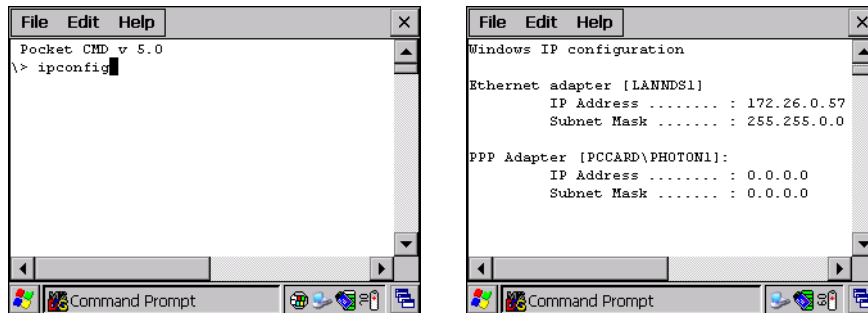


Figure 2-7 Ethernet IP Address

Charging and Communication

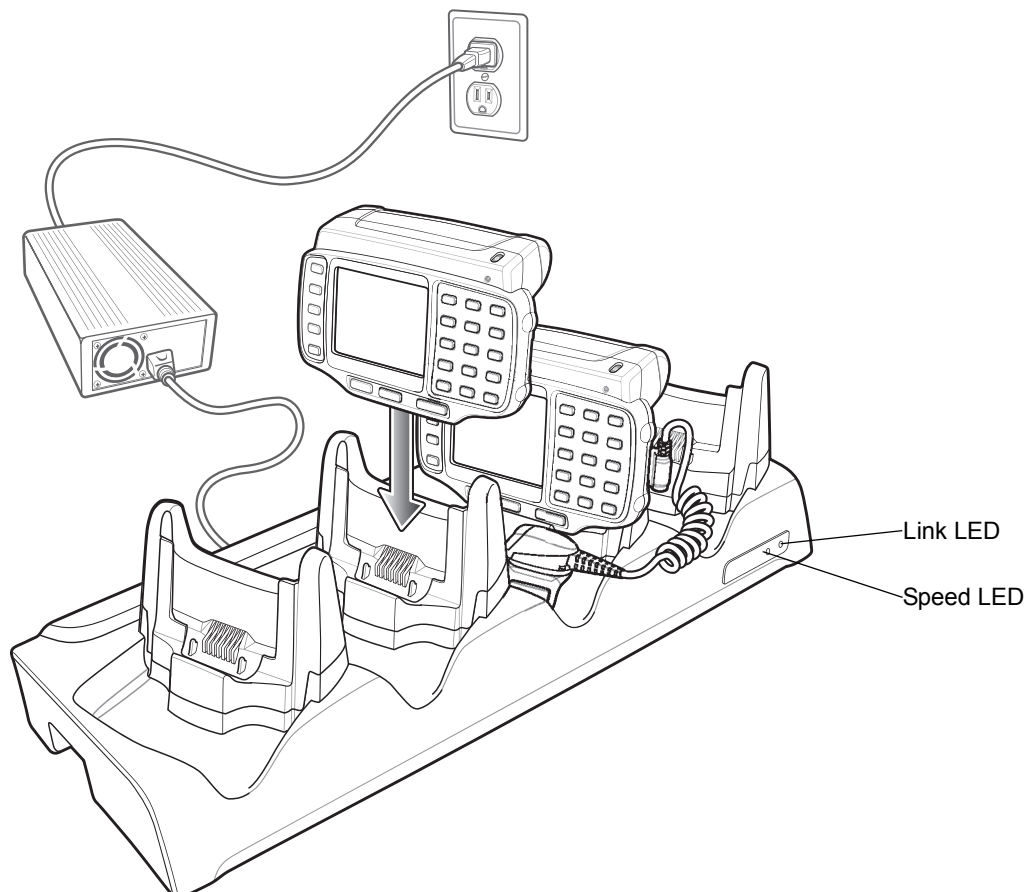


Figure 2-8 Four Slot Ethernet Cradle

Battery Charging Indicators

The wearable terminal's amber Charge Status LED shows the status of the battery charging in the wearable terminal. See [Table 1-2 on page 1-5](#) for charging status indications. The standard capacity battery usually charges in less than four hours and the extended capacity battery usually charges in less than eight hours.

Speed LED

The green Speed LED lights to indicate that the transfer rate is 100 Mbps. When the LED is not lit the transfer rate is 10Mbps.

Link LED

The yellow Link LED blinks to indicate activity, or stays lit to indicate that a link is established. When it is not lit it indicates that there is no link.

Four Slot Spare Battery Charger



CAUTION Ensure that you follow the guidelines for battery safety described in [Battery Safety Guidelines on page 10-3](#).

This section describes how to set up and use the Four Slot Spare Battery Charger to charge up to four spare batteries.

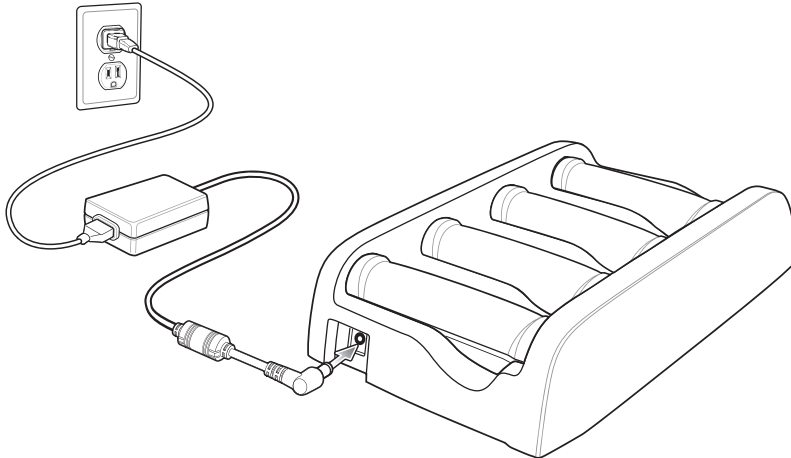


Figure 2-9 Four Slot Spare Battery Charger Setup



CAUTION Use only an approved power supply output rated 12 VDC and minimum 3.3 A. Use of an alternative power supply will void the product warranty and may cause product damage. Refer to the *WT4070/90 User Guide* for the power supply regulatory compliance statement.

Spare Battery Charging

1. Connect the charger to a power source.
2. Insert the battery into a spare battery charging slot and press down on the battery to ensure proper contact.

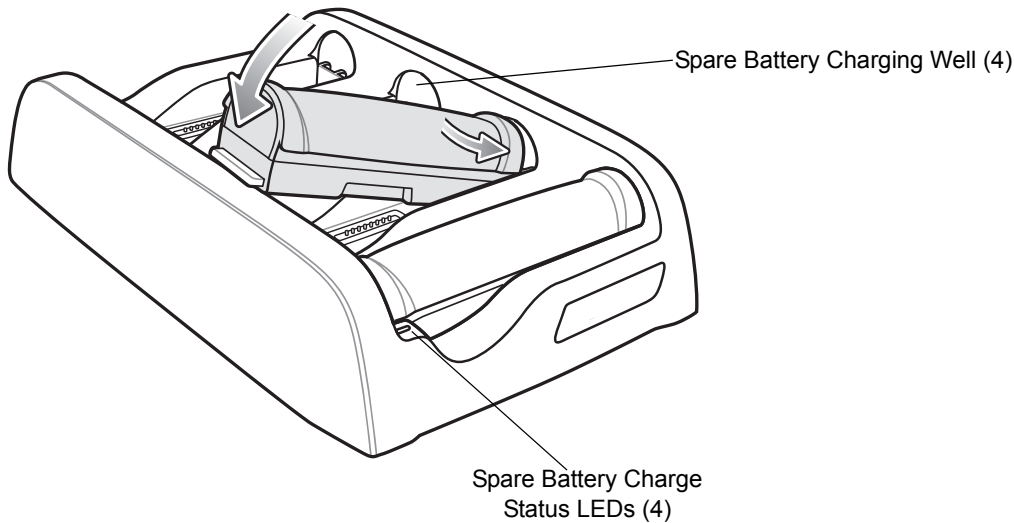


Figure 2-10 Spare Battery Charging

Battery Charging Indicators

Each battery charging well has an amber Spare Battery Charge Status LED. (see [Figure 2-10 on page 2-11](#)). See [Table 2-2](#) for charging status indications.

The standard capacity battery usually charges in less than four hours and the extended capacity battery usually charges in less than eight hours.

Table 2-2 Spare Battery Charge Status LED Indicators

LED	Indication
Off	No spare battery in slot; spare battery not placed correctly; cradle is not powered.
Fast Blinking Amber	Charging error: <ul style="list-style-type: none">• Temperature is too low or too high.• Charging has gone on too long without completing (typically eight hours).
Slow Blinking Amber	Spare battery is charging.
Solid Amber	Charging complete.

Wall Mount Bracket

Use the wall mounting bracket to mount a Four Slot Ethernet cradle and a Four Slot Battery Charge together on a wall.

To mark the screw holes for mounting the bracket use the wall mounting bracket as a template. Place the bracket onto the wall, level and mark the five screw hole locations.

1. Install top three screws into the wall.
2. Align the top three mounting holes with the screws.
3. Place mounting bracket on screws.
4. Secure the mounting bracket to the wall by tightening the three screws.
5. Install and secure two screws at the bottom of the bracket.

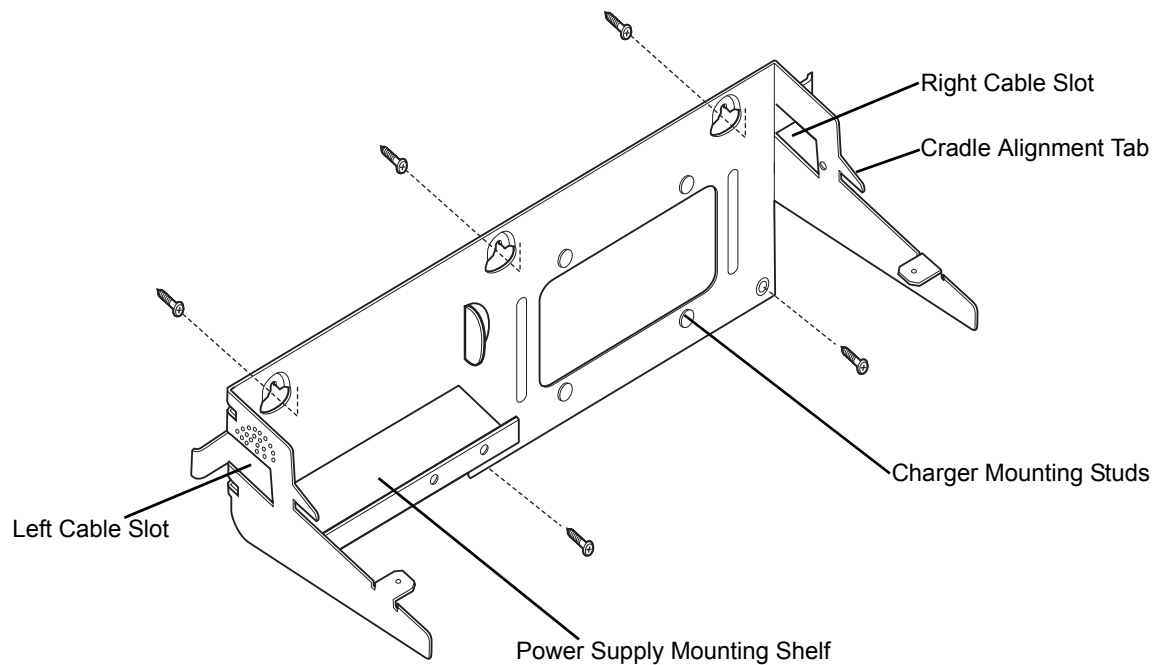


Figure 2-11 *Mounting the Bracket*

Power Supply Installation

Place power supply onto mounting shelf with the DC output connector and fan facing out and with the fan on top.

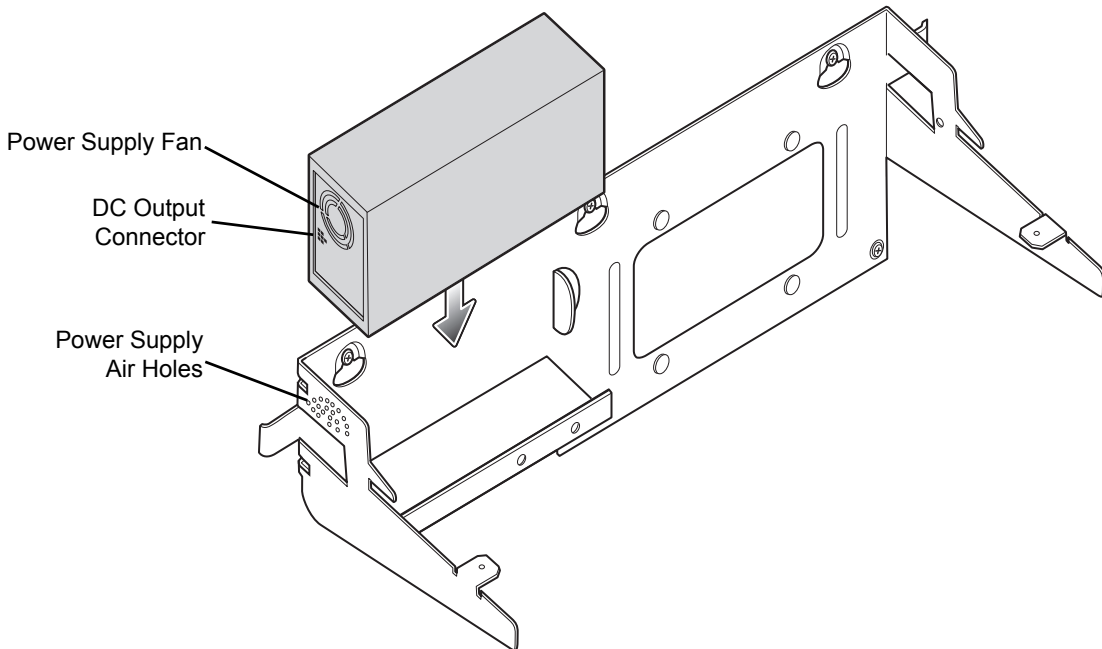


Figure 2-12 *Installing the Power Supply*

Four Slot Ethernet Cradle Installation

1. Align the two slots in the back of the cradle with the two cradle alignment tabs on the bracket.

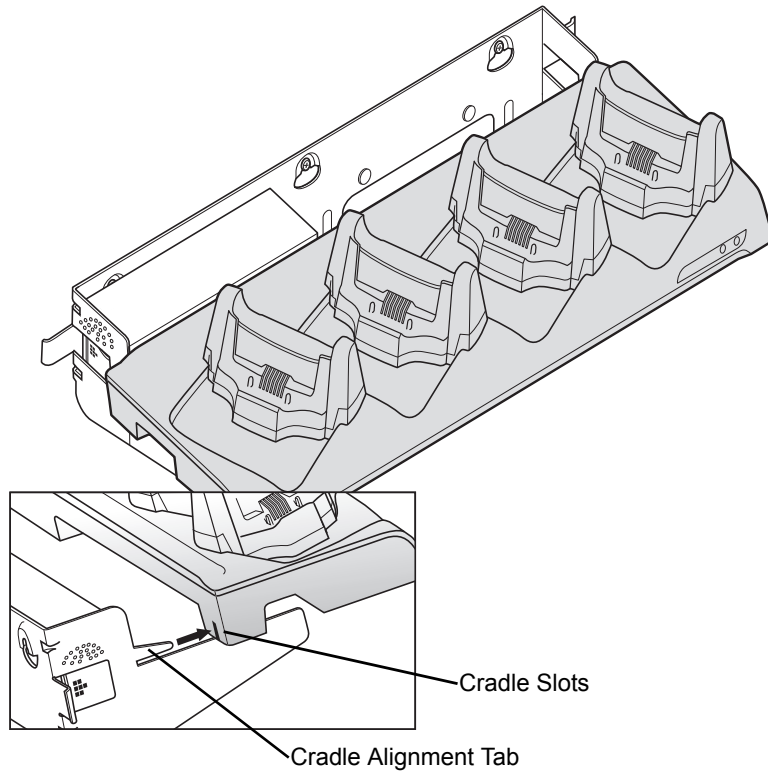


Figure 2-13 *Aligning the Slots in the Cradle with Mounting Bracket Tabs*

2. Secure the cradle to the mounting bracket with two M4.0 screws supplied with the bracket.

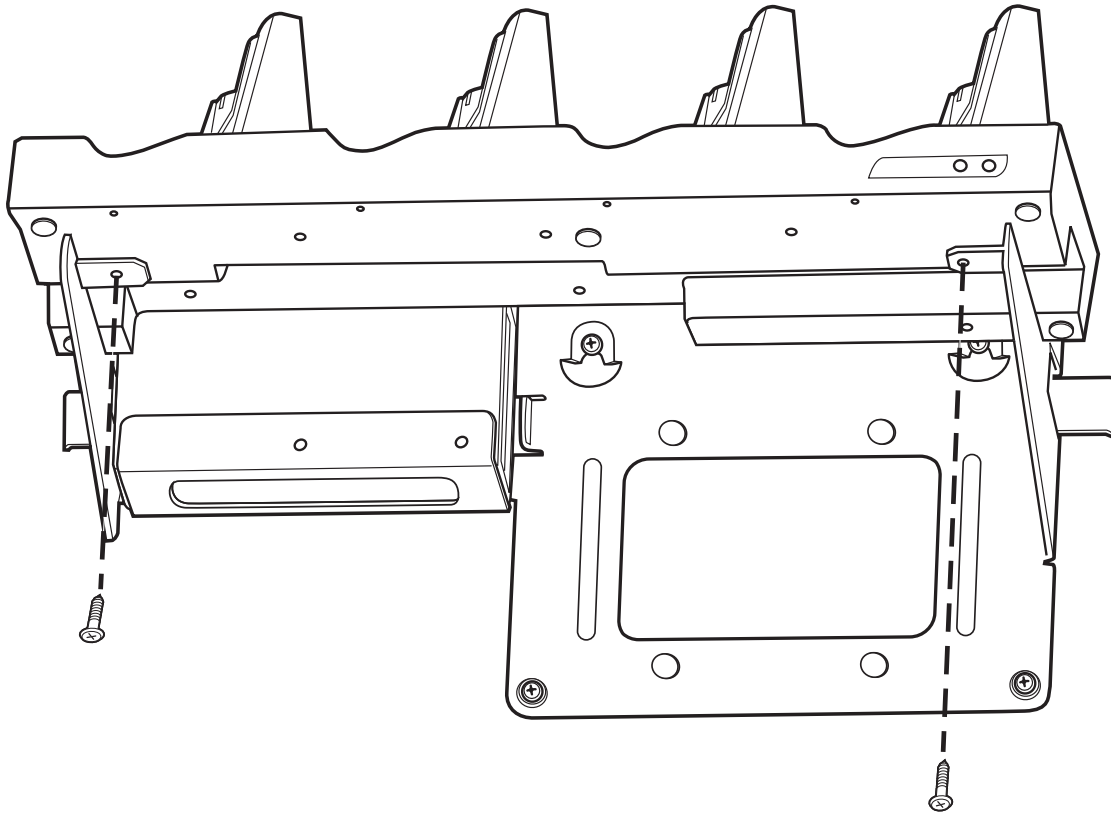


Figure 2-14 *Securing the Four-Slot Ethernet Cradle to the Mounting Bracket*

Four Slot Battery Charger Installation

The Four Slot Spare Battery Charger has four mounting slots on the back. Around the slots are guides that assist in proper alignment of the charger onto the mounting bracket. Gravity holds the charger in place.

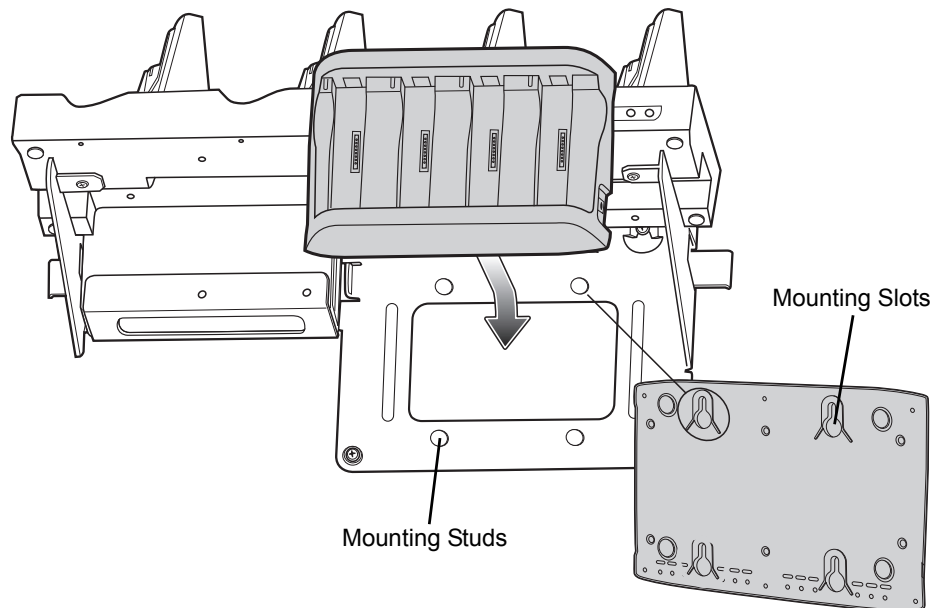


Figure 2-15 *Installing the Battery Charger onto the Mounting Bracket*

Position the charger over the mounting studs and slide the charger into place.

Ensure that the charger is seated properly.

Wiring

The AC line cord provides AC power to the power supply. The mounting bracket power cable provides power from the power supply to the Four Slot Ethernet cradle and the Four Slot Spare Battery Charger. Ethernet cables (not supplied) connects the cradle to the local network and to another cradle, if required.

Ensure that the AC line cord is long enough to reach from the AC power source to the power supply.

1. Route the AC line cord through the right cable slot of the bracket.
2. Plug the AC line cord into the power supply AC input connector.
3. Route the power supply connector of the power cable through the cradle channel and out the left side of the cradle.
4. Plug the power cable connector into the DC output connector on the power supply.
5. Plug the cradle power plug into the Four Slot Ethernet cradle input power connector.
6. Plug the charger power plug onto the Four Slot Spare battery Charger input power connector.
7. Plug one end of the Ethernet cable into the appropriate connector on the Four Slot Ethernet cradle.
8. Route the cables as shown in [Figure 2-16](#) and [Figure 2-17](#).
9. Use two tie-wraps to secure the power cable Y connection to the power supply mounting shelf.

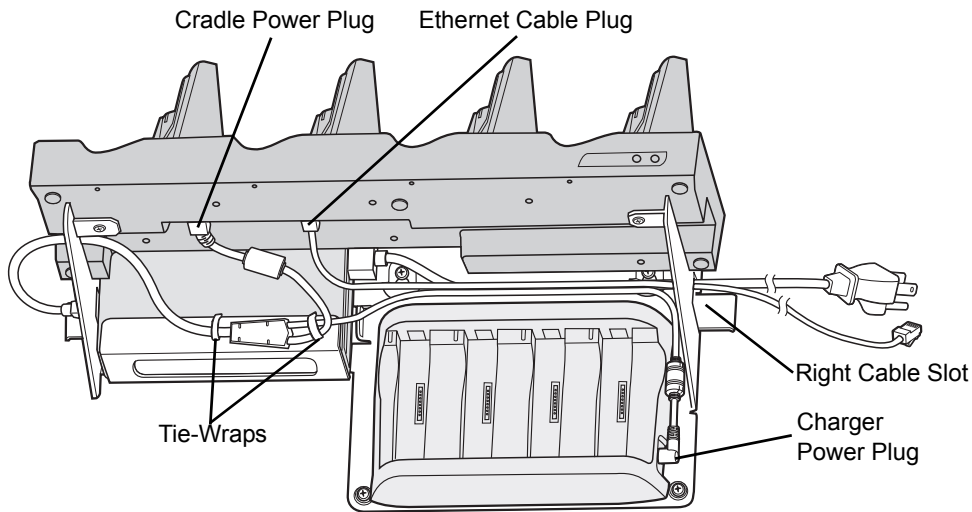


Figure 2-16 Cable Routing

10. Use one tie-wrap to secure the AC line cord and Ethernet cable to the mounting bracket.
11. Use two tie-wraps to secure the charger power lead, the AC line cord and Ethernet cable (if required) together as shown below.

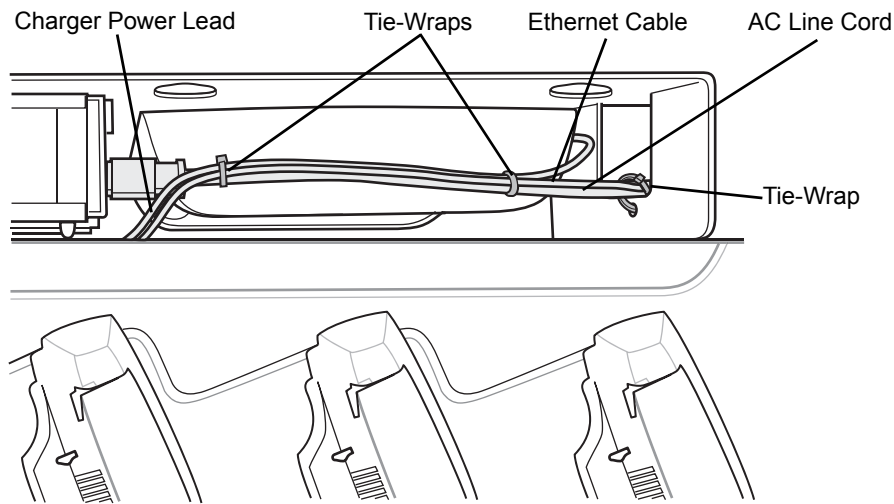


Figure 2-17 Routing Cables

12. Plug the AC line cord into an AC power source.

Placing a Battery in the Charger

When placing a spare battery into the Four Slot Spare Battery Charger, ensure proper orientation of the battery.

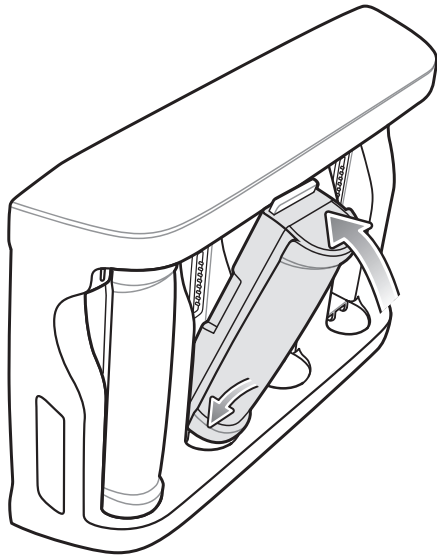


Figure 2-18 *Inserting a Battery into the Battery Charger*

Mounting Multiple Brackets

When installing multiple brackets on a wall:

- Each mounting bracket must be 25.4 cm (10 in.) from the top of one bracket to the top of the next bracket.
- The bottom of the last bracket must be at least 61 cm (24 in.) from the floor.
- When mounting brackets next to each other the tabs must at least touch each other to ensure minimum distance between brackets.

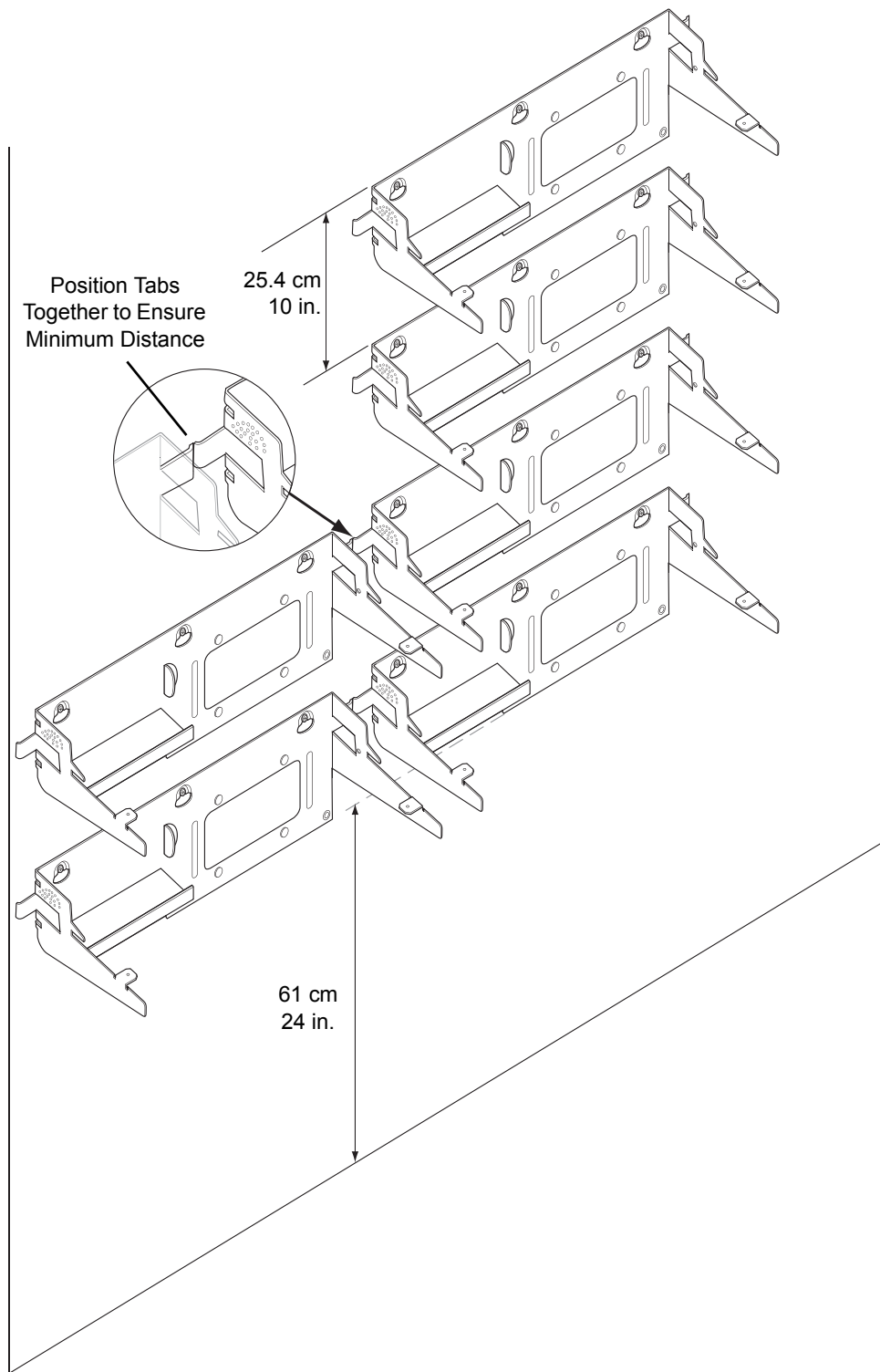


Figure 2-19 *Installing Multiple Mounting Brackets*

Navigating the Wearable Terminal with an External Input Device

To assist in development, an external input device, such as a mouse, can be used to navigate the desktop and applications instead of using the wearable terminal keypad.

- USB devices
 - mouse
 - keyboard
 - hub
- Bluetooth mouse.

USB Device

✓ **NOTE** The wearable terminal must be inserted into the Single Slot USB cradle to use a USB input device.

The following is required to connect a USB device:

- a commercially-available USB cable or Zebra's USB Adapter with a mini USB A connector on one end and a USB A Female connector on the other end.
- a USB device
 - a USB keyboard
 - a USB mouse
 - a USB hub (optional).

Connect the mini USB A connector end into the USB connector on the back of the Single Slot USB cradle. The cradle automatically detects the USB A connector and places the wearable terminal into USB host mode. Connect the USB device (mouse or keyboard) connector into the USB A Female connector. You can also connect both a mouse and keyboard to a hub and the hub to the USB A Female connector.

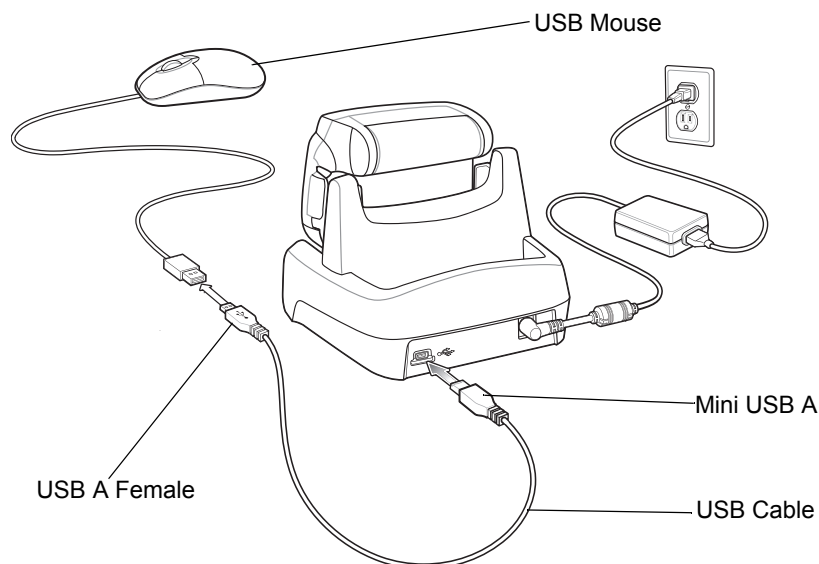


Figure 2-20 USB Mouse Connection to the Single Slot USB Cradle

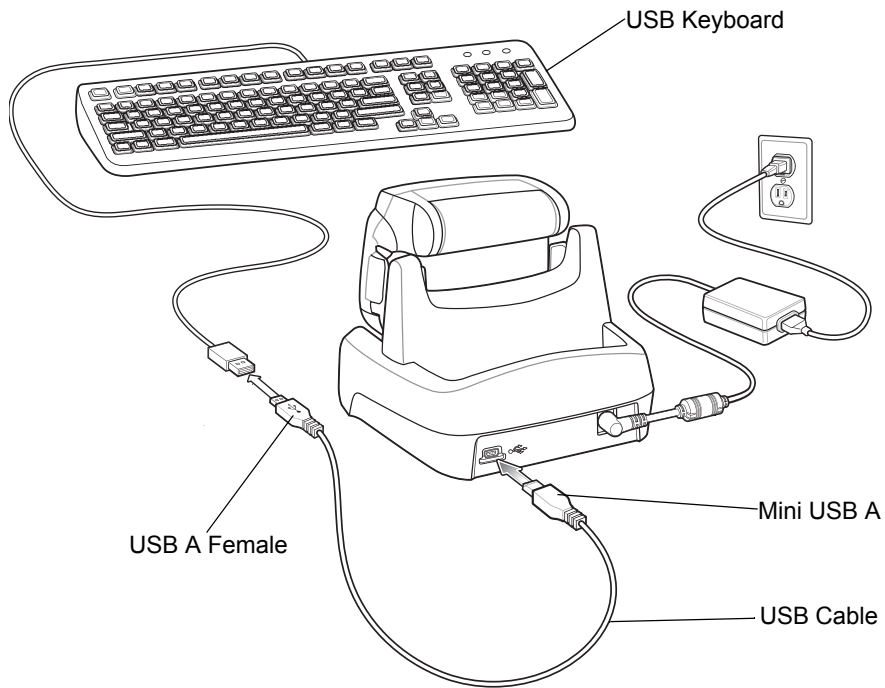


Figure 2-21 *USB Keyboard Connection to the Single Slot USB Cradle*

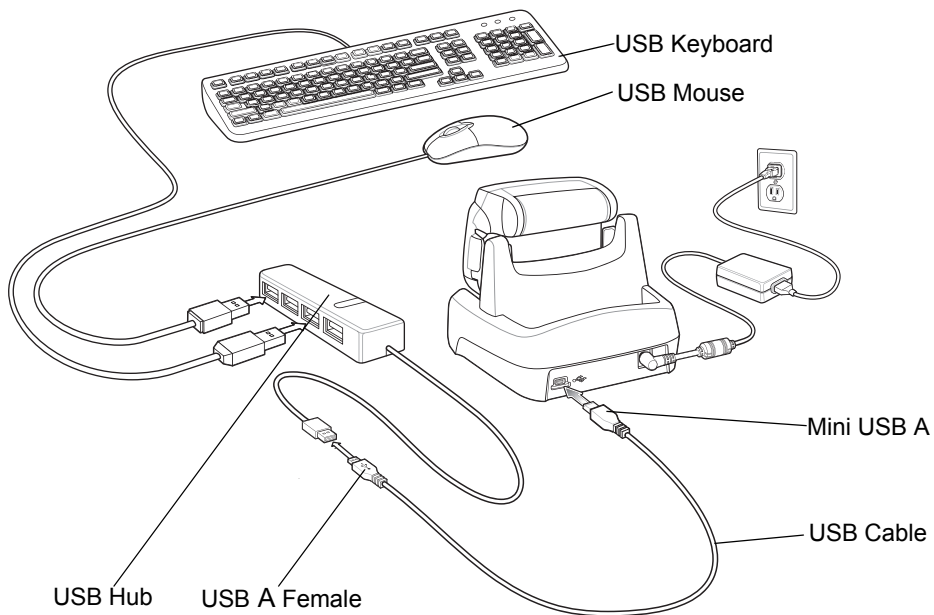


Figure 2-22 *USB Mouse/Keyboard/Hub Connection to the Single Slot USB Cradle*

Bluetooth Mouse

✓ **NOTE** The following procedures assume that you are using the wearable terminal keypad.

Use these procedures for OEM version 04.20.0004 and below.

For OEM version 05.30.0000 and above, see [Chapter 6, Using Bluetooth](#) for more information on using the BTEplorer application.

To setup a Bluetooth mouse:

1. If the Start Up window is not displayed, open the Start Up menu (OTL).
2. Press **5**.
3. Press **3**. The **StackHID** window displays.
4. Press **ALT - ALT** to access the file menu.
5. Use the navigation keys and select **Setup > Port > BTS6**. Press **ENTER**. The large text box displays the stack initializing. The text ends with the word "success".
6. Place the Bluetooth mouse into *Discovery* mode (refer to the instruction manual for the mouse).
7. Press **ALT - ALT** to access the file menu.
8. Use the navigation keys and select **Devices > Start Inquiry**. Press **ENTER**. The wearable terminal searches for Bluetooth devices in the area and displays the Bluetooth address for each Bluetooth device it discovers in the text below the large text box.
9. To get more information about a particular discovered Bluetooth device press **TAB** to highlight the Bluetooth addresses listed in the text box.
10. Use the navigation keys to select a particular Bluetooth address.
11. Press **ALT - ALT** to access the file menu.
12. Use the navigation keys to select **Devices > Get Remote Device Name**. Press **ENTER**.
13. The wearable terminal communicates with the Bluetooth device and then displays the device name in the large text box. For example, it may display *Microsoft Mouse*.
14. Once you know which Bluetooth address belongs to the Bluetooth mouse you wish to connect to, highlight that Bluetooth address.
15. Press **ALT - ALT** to access the file menu.
16. Use the navigation keys and select **Remote Data > Send to OS**. Press **ENTER**.
17. Press the **TAB** key continuously until the **Open Client** button is highlighted.
18. Press **ENTER**.
19. The wearable terminal connects to the Bluetooth mouse.
20. Do not close the **StackHID** window. Closing the window disables the Bluetooth HID connection.

Connector Shroud

Assembly

1. Remove cable from wearable terminal, if required.
2. Align the cable connector with the connector shroud bottom housing. Ensure that the disconnect button on the connector faces up.

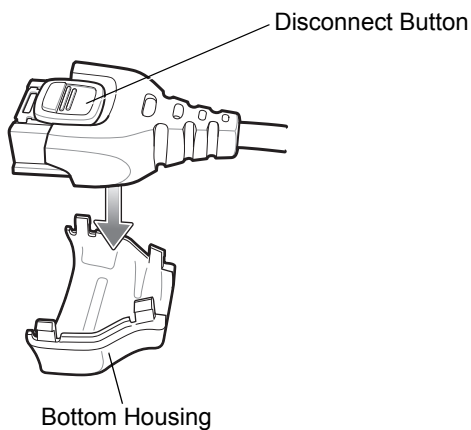


Figure 2-23 *Installing Bottom Housing*

3. Place the cable connector into the shroud bottom housing as shown.

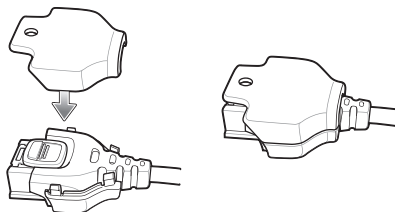


Figure 2-24 *Installing Top Housing*

4. Press the top housing into the bottom housing. The housings will snap together.
5. Plug the cable connector into the wearable terminal connector.

Disconnecting the Cable from the Wearable Terminal

✓ **NOTE** Follow the instructions below when disconnecting the cable connector and shroud from the wearable terminal. Once the shroud is installed on the connector, do not disassemble the shroud by prying it apart.

1. Turn the wearable terminal over to expose the top housing of the shroud.
2. Push the tip of a ball-point pen through the hole in the connector shroud top housing. The connector disengages from the wearable terminal.

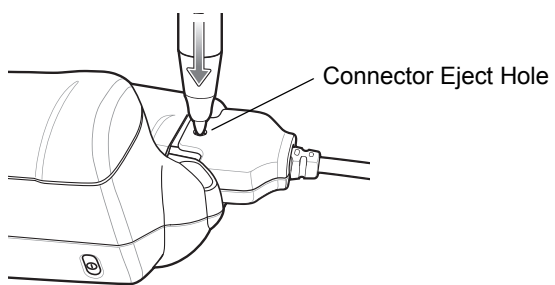


Figure 2-25 *Disconnecting Connector with Shroud*

Chapter 3 ActiveSync

Introduction

To communicate with various host devices, install Microsoft ActiveSync (version 4.1 or higher) on the host computer. Use ActiveSync to synchronize information on the wearable terminal with information on the host computer. Changes made on the wearable terminal or host computer appear in both places after synchronization.

ActiveSync software:

- Allows working with wearable terminal-compatible host applications on the host computer. ActiveSync replicates data from the wearable terminal so the host application can view, enter, and modify data on the wearable terminal.
- Synchronizes files between the wearable terminal and host computer, converting the files to the correct format.
- Backs up the data stored on the wearable terminal. Synchronization is a one-step procedure that ensures the data is always safe and up-to-date.
- Copies (rather than synchronizes) files between the wearable terminal and host computer.
- Controls when synchronization occurs by selecting a synchronization mode, e.g., set to synchronize continually while the wearable terminal is connected to the host computer, or set to only synchronize on command.
- Selects the types of information to synchronize and controls how much data is synchronized.

Installing ActiveSync

To install ActiveSync on the host computer, download version 4.1 or higher from the Microsoft web site at <http://www.microsoft.com>. Refer to the installation included with the ActiveSync software.

Wearable Terminal Setup

- ✓ **NOTE** Microsoft recommends installing ActiveSync on the host computer before connecting the wearable terminal.

The wearable terminal is set by default to communicate using a USB connection. [Chapter 2, Accessories](#) provides the accessory setup and cable connection information for use with the wearable terminal. The wearable terminal communication settings must be set to match the communication settings used with ActiveSync.

Setting Up an ActiveSync Connection on the Host Computer

- ✓ **NOTE** The normal function of the product may be disturbed by Strong Electro Magnetic Interference (for example, static electricity). If so, simply remove and re-insert the terminal to resume normal operation. In case the function does not resume, please use the product in another location.

To start ActiveSync:

1. Select **Start > Programs > Microsoft ActiveSync** on the host computer. The **ActiveSync** Window displays.

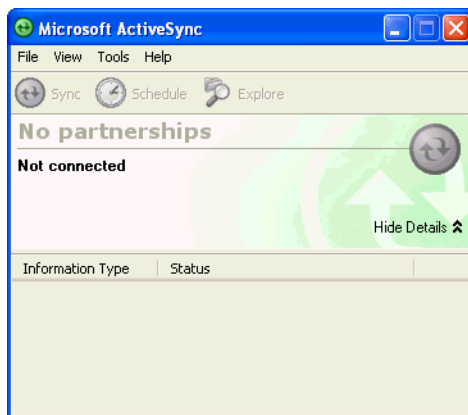


Figure 3-1 ActiveSync Window

- ✓ **NOTE** Assign each wearable terminal a unique device name. Do not try to synchronize more than one wearable terminal to the same name.

2. In the **ActiveSync** window, select **File > Connection Settings**. The **Connection Settings** window appears.



Figure 3-2 Connection Settings Window

3. Select **Allow USB connections** check box.
4. Select the **Show status icon in Taskbar** check box.
5. Select **OK** to save any changes made.

Setting up a Partnership

To set up a partnership:

1. If the **Get Connected** window does not appear on the host computer, select **Start > All Programs > Microsoft ActiveSync**.

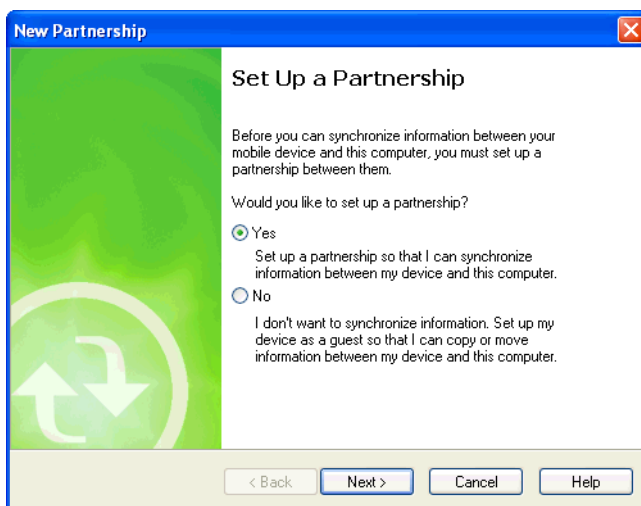


Figure 3-3 New Partnership Window

2. Select if you want to synchronize with the host computer or to connect as a guest.
3. Click **Next**.

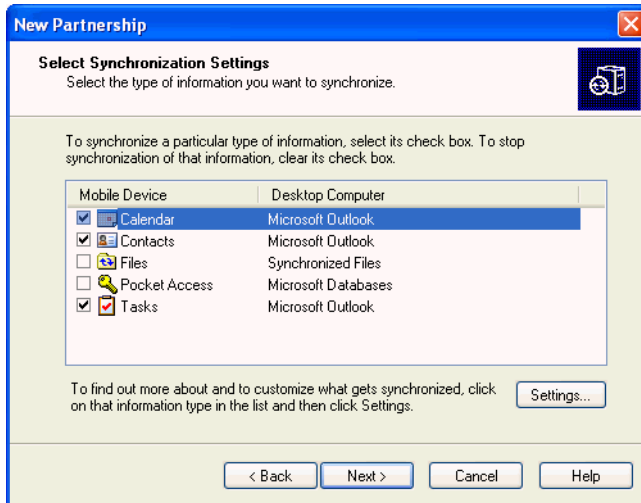


Figure 3-4 Select Synchronization Setting Window

4. Select the appropriate settings and click **Next**.

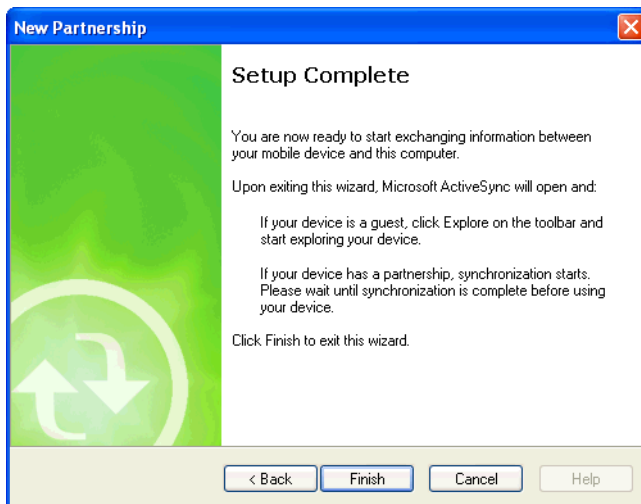


Figure 3-5 Setup Complete Window

5. Click **Finish**.

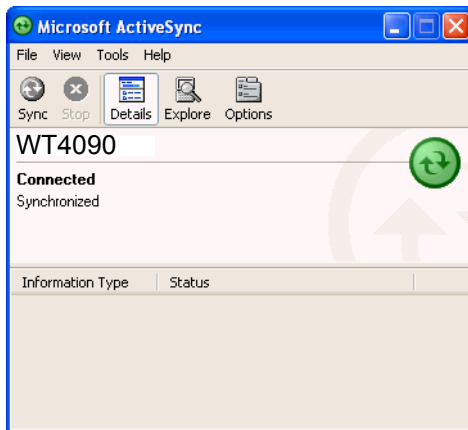


Figure 3-6 *ActiveSync Connected Window*

During the first synchronization, information stored on the wearable terminal is copied to the host computer. When the copy is complete and all data is synchronized, the wearable terminal can be disconnected from the host computer.

- ✓ **NOTE** The first ActiveSync operation must be performed with a local, direct connection. To retain partnerships after a cold boot, capture partnership registry information in a .reg file and save it in the Flash File System, See the detailed information provided in the SMDK Windows Help File.

For more information about using ActiveSync, start ActiveSync on the host computer, then see ActiveSync Help.

Chapter 4 Voice Only WT4090 Remote Control

Introduction

Since the Voice Only WT4090 does not have a display, access to settings and controls must be done using a remote display software, such as MotoRC or ActiveSync Remote Display.

MotoRC Software

Download the MotoRC application from the Zebra Support Central web site: <http://www.zebra.com/support>. Follow the instructions provided with the software to install on a host computer.

Microsoft ActiveSync Remote Display Software

Download Windows Mobile Power Toys from the Microsoft web site: <http://www.microsoft.com>. Follow the instructions with the software to install on a host computer.

Ensure that ActiveSync is installed on the host computer. See [Chapter 3, ActiveSync](#) for more information.

Connection to Host Computer

To connect the Voice Only WT4090 to a host computer:

1. Connect the Single Slot Serial/USB cradle to the host computer. See [Single Slot USB Cradle on page 2-2](#) for setup instructions.
2. Insert the Voice Only WT4090 into the cradle.
3. If ActiveSync was installed properly, the host computer automatically detects the Voice Only WT4090 and begins ActiveSync. The **ActiveSync** window appears.
4. Select the **Yes** radio button to create a partnership with the host computer or select **No** radio button to connect as a guest.
5. Click **Next**. The **Microsoft ActiveSync** window indicates that it is connected to the Voice only WT4090.

MotoRC Connection

To control the Voice Only WT4090 using the MotoRC software:

1. On the host computer, click **Start > Programs > MSP > MotoRC > Run Remote Control**. The **Run Remote Control** DOS window opens followed by the **Remote Control** window.

UI Control Icon

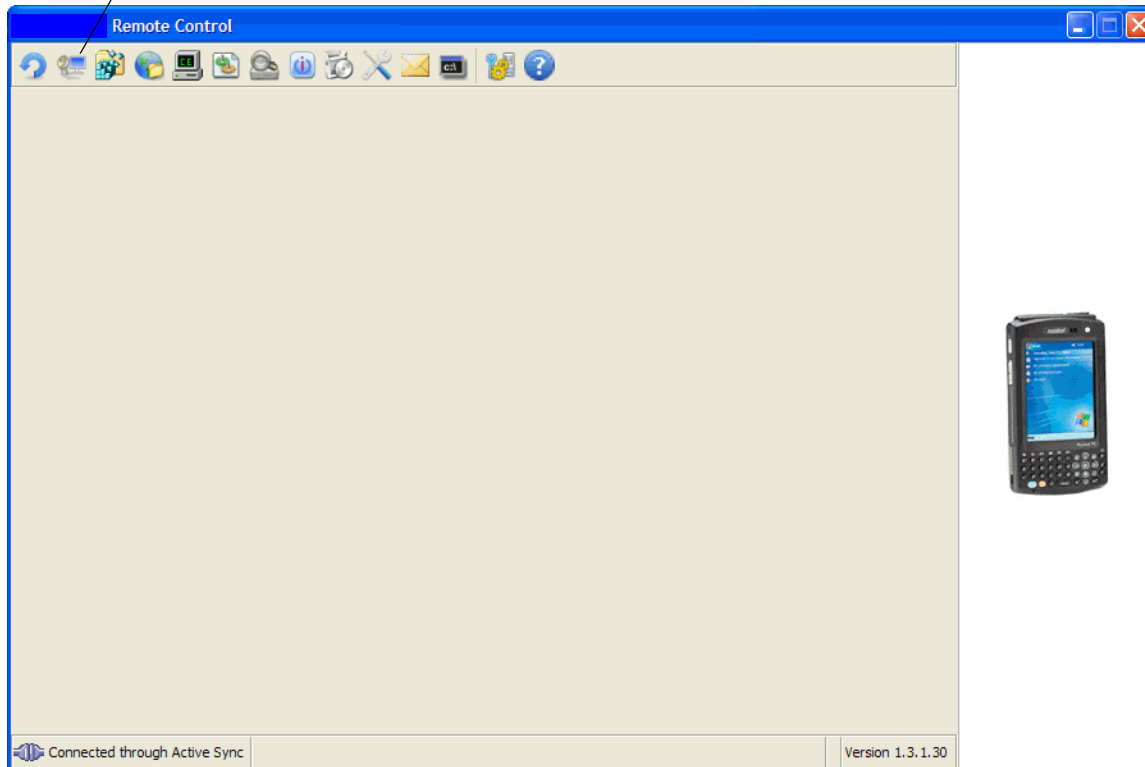


Figure 4-1 Remote Control Window

2. Click on the **UI Control** icon to display the Voice Only WT4090 desktop.

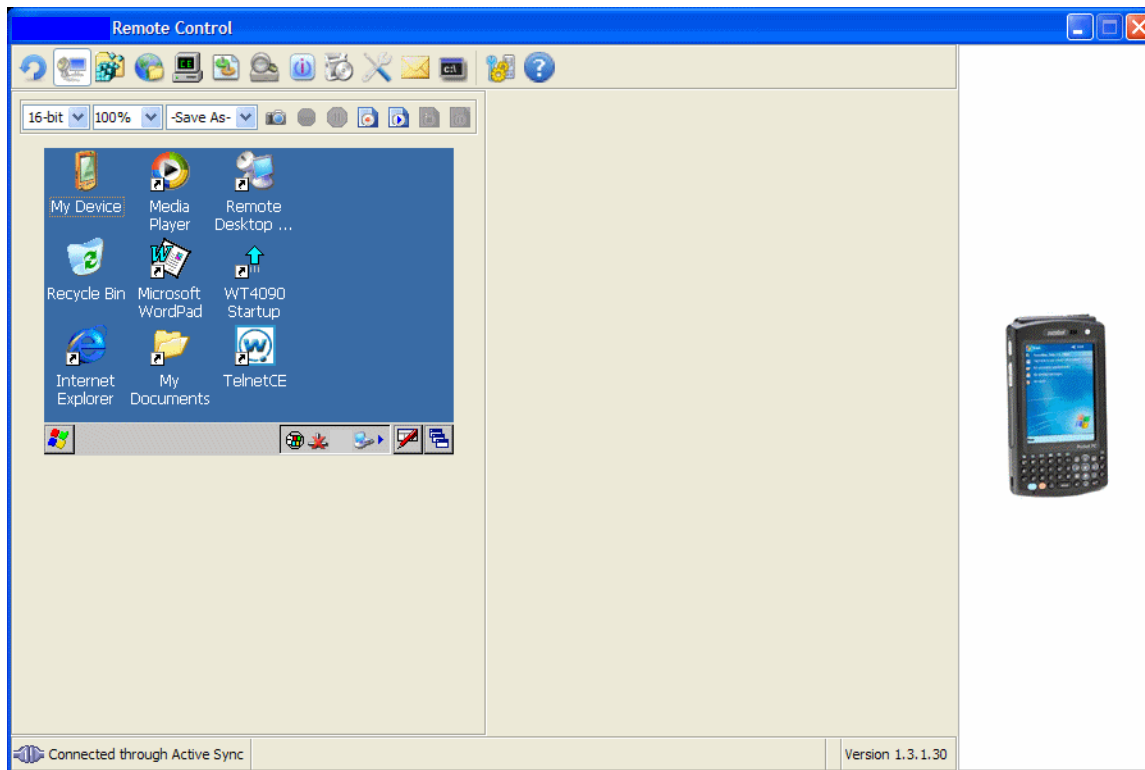


Figure 4-2 Remote Control Window with Voice Only WT4090 Desktop

3. Use the host computer mouse to control the Voice Only WT4090 desktop.
4. When finished, close the **Remote Control** and **Run Remote Control** windows.

Microsoft ActiveSync Remote Display Connection

To control the Voice Only WT4090 using the Microsoft ActiveSync Remote Display software:

1. On the host computer, click **Start > Programs > ActiveSync Remote Display**. The **ActiveSync Remote Display** window displays with the Voice Only WT4090 desktop shown.



Figure 4-3 ActiveSync Remote Display Window

2. Use the host computer mouse to control the Voice Only WT4090 desktop.
3. When finished, close the **ActiveSync Remote Display** window.

Chapter 5 Wireless Applications

Introduction

- ✓ **NOTE** This chapter described Fusion versions below 2.55. For Fusion versions 2.55 and above, refer to the *Wireless Fusion Enterprise Mobility Suite User Guide for Version X.XX User Guide* for information, where X.XX represents the Fusion version number. These guides are available on the Zebra Support Central web site: <http://www.zebra.com/support>.

Wireless Local Area Networks (LANs) allow wearable terminals to communicate wirelessly and send captured data to a host device in real time. The wearable terminal supports the IEEE 802.11a (WT4090 only), 802.11b and 802.11g standards. Before using the wearable terminal on a WLAN, the facility must be set up with the required hardware to run the wireless LAN and the wearable terminal must be configured. Refer to the documentation provided with the access points (APs) for instructions on setting up the hardware.

To configure the wearable terminal, a set of wireless applications provide the tools to configure and test the wireless radio in the wearable terminal. The **Wireless Application** menu on the task tray provides the following wireless applications:

- Wireless Status
- Wireless Diagnostics
- Find WLANs
- Manage Profiles
- Options
- Log On/Off
- Enable/Disable Radio.

Press **ALT - w** to display the **Wireless Applications** menu.

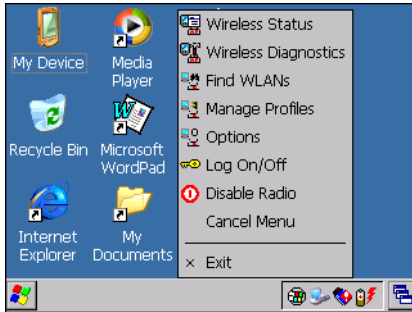


Figure 5-1 *Wireless Applications Menu*

Signal Strength Icon

The **Signal Strength** icon in the task tray indicates the wearable terminal's wireless signal strength as follows:

Table 5-1 *Wireless Applications Icons, Signal Strength Descriptions*

Icon	Status	Action
	Excellent signal strength	Wireless LAN network is ready to use.
	Very good signal strength	Wireless LAN network is ready to use.
	Good signal strength	Wireless LAN network is ready to use.
	Fair signal strength	Wireless LAN network is ready to use. Notify the network administrator that the signal strength is only "Fair".
	Poor signal strength	Wireless LAN network is ready to use. Performance may not be optimum. Notify the network administrator that the signal strength is "Poor".
	Out-of-network range (not associated)	No wireless LAN network connection. Notify the network administrator.
	No wireless LAN network card detected	No wireless LAN network card detected or radio disabled. Notify the network administrator.

Turning the WLAN Radio On and Off

To turn off the WLAN radio:

1. Press **ALT - w**. The Wireless menu appears.
2. Using the navigation keys, select **Disable Radio**.
3. Press **ENTER**.

To turn on the radio:

1. Press **ALT - w**. The Wireless menu appears.
2. Using the navigation keys, select **Enable Radio**.
3. Press **ENTER**.

Find WLANs Application

Use the **Find WLANs** application to discover available networks in the vicinity of the user and wearable terminal. To open the **Find WLANs** application:

1. Press **ALT - w**. The Wireless menu appears.
2. Using the navigation keys, select **Find WLANs**.
3. Press **ENTER**. The **Find WLANs** window displays.

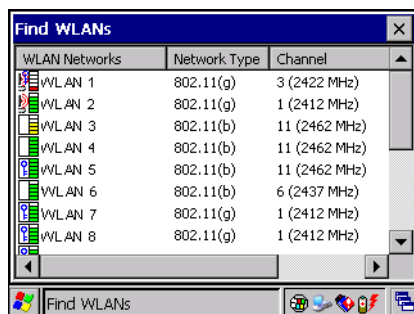


Figure 5-2 Find WLANs Window



NOTE The **Find WLANs** display is limited to 32 items (ESSIDs or MAC addresses). A combination of up to 32 ESSIDs/APs may be displayed.

Manually enter valid ESSIDs not displayed in the **Find WLANs** window. See [Figure 4-5 on page 4-6](#).

The **Find WLANs** list displays:

- **WLAN Networks** - Available wireless networks with icons that indicate signal strength and encryption type. The signal strength and encryption icons are described in [Table 4-1](#) and [Table 4-3](#).
- **Network Type** - Type of network.
- **Channel** - Channel on which the AP is transmitting.
- **Signal Strength** - The signal strength of the signal from the AP.

Table 5-2 *Signal Strength Icon*










Icon	Description
	Excellent signal
	Very good signal
	Good signal
	Fair signal
	Poor signal
	Out of range or no signal

Table 5-3 *Encryption Icon*

Icon	Description
	No encryption. WLAN is an infrastructure network.
	WLAN is an Ad-Hoc network.
	WLAN access is encrypted and requires a password.

Select a WLAN network in the list using the navigation keys. Press **ALT - m** to open a pop-up menu which provides two options: **Connect** and **Refresh**. Select **Refresh** and press **ENTER** to refresh the WLAN list. Select **Connect** and press **ENTER** to create a wireless profile from that network. This starts the **Profile Editor Wizard** which allows you to set the values for the selected network. After editing the profile, the wearable terminal automatically connects to this new profile.

Profile Editor Wizard

Use the **Profile Editor Wizard** to create a new profile or edit an existing profile. If editing a profile, the fields reflect the current settings for that profile. If creating a new profile, the known information for that WLAN network appears in the fields.

Navigate through the wizard using the **Next** and **Back** buttons. Press **ESC** to quit. On the confirmation dialog box, select **No** to return to the wizard or select **Yes** to quit and return to the **Manage Profiles** window. See [Manage Profiles Application on page 5-22](#) for instructions on navigating the **Profile Editor Wizard**.

Profile ID

In the **Profile ID** dialog box in the **Profile Editor Wizard**, enter the profile name and the ESSID.

1. Enter a new name for the profile in the **Name** text box.
2. Press **TAB**.
3. In the **ESSID** text box, enter a name for the ESSID.
4. Press **TAB**. The **Next** button highlights.



Figure 5-3 Profile ID Dialog Box

Table 5-4 Profile ID Fields

Field	Description
Name	The name and (WLAN) identifier of the network connection. Enter a user friendly name for the wearable terminal profile used to connect to either an AP or another networked computer. Example: The Public LAN.
ESSID	The ESSID is the 802.11 extended service set identifier. The ESSID is a 32-character (maximum) string identifying the WLAN, and must match the AP ESSID for the wearable terminal to communicate with the AP.

✓ **NOTE** Two profiles with the same user friendly name are acceptable but not recommended.

5. Press **ENTER**. The **Operating Mode** dialog box displays.

Operating Mode

Use the **Operating Mode** dialog box to select the operating mode (Infrastructure or Ad-Hoc) and the country location.

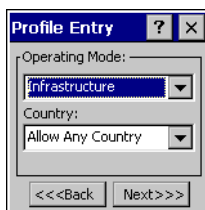


Figure 5-4 Operating Mode Dialog Box

1. Use the navigation keys to select the operating mode.
2. Press **TAB**.
3. Up the navigation keys to select the country.
4. Press **TAB** twice. The **Next** button highlights.

Table 5-5 *Operating Mode Fields*

Field	Description
Operating Mode	<p>Select Infrastructure to enable the wearable terminal to transmit and receive data with an AP. Infrastructure is the default mode.</p> <p>Select Ad Hoc to enable the wearable terminal to form its own local network where wearable terminals communicate peer-to-peer without APs using a shared ESSID.</p>
Country	<p>Country determines if the profile is valid for the country of operation. The profile country must match the country in the options page or it must match the acquired country if 802.11d is enabled.</p> <p>Single Country Use: When the device is only used in a single country, set every profile country to Allow Any Country. In the Options > Regulatory dialog box (see Regulatory Options on page 5-34), select the specific country the device is used in, and deselect the Enable 802.11d option. This is the most common and efficient configuration, eliminating the initialization overhead associated with acquiring a country via 802.11d.</p> <p>Multiple Country Use: When the device is used in more than one country, select the Enable 802.11d option in the Options > Regulatory dialog box (see Regulatory Options on page 5-34). This eliminates the need for reprogramming the country (in Options > Regulatory) each time you enter a new country. However, this only works if the infrastructure (i.e., APs) supports 802.11d (some infrastructures do not support 802.11d, including some Cisco APs). When the Enable 802.11d option is selected, the Options > Regulatory > Country setting is not used. For a single profile that can be used in multiple countries, with infrastructure that supports 802.11d (including Zebra infrastructure), set the Profile Country to Allow Any Country. Under Options > Regulatory, select Enable 802.11d. The Options > Regulatory > Country setting is not used.</p> <p>For a single profile that can be used in multiple countries, but with infrastructure that does not support 802.11d, set the profile country to Allow Any Country, and de-select (uncheck) Enable 802.11d. In this case, the Options > Regulatory > Country setting must always be set to the country the device is currently in. This configuration option is the most efficient and may be chosen for use with any infrastructure. However, the Options > Regulatory > Country setting must be manually changed when a new country is entered. Note that using a single profile in multiple countries implies that there is a common ESSID to connect to in each country. This is less likely than having unique ESSIDs in each country, this requires unique profiles for each country.</p> <p>For additional efficiency when using multiple profiles that can be used in multiple countries, the country setting for each profile can be set to a specific country. If the current country (found via 802.11d or set by Options > Regulatory > Country when 802.11d is disabled) does not match the country set in a given profile, then that profile is disabled. This can make profile roaming occur faster. For example, if two profiles are created and configured for Japan, and two more profiles are created and configured for USA, then when in Japan only the first two profiles are active, and when in USA only the last two are active. If they had all been configured for Allow Any Country, then all four would always be active, making profile roaming less efficient.</p>

5. Press **ENTER**. If **Ad-Hoc** mode was selected the **Ad-Hoc** dialog box displays. If **Infrastructure** mode was selected the **Authentication** dialog box displays. See [Authentication on page 4-9](#) for instruction on setting up authentication.

Ad-Hoc

Use the **Ad-Hoc** dialog box to select the required information to control **Ad-Hoc** mode. This dialog box does not appear if you selected **Infrastructure** mode. To select Ad-Hoc mode:

1. Press **Tab** to highlight the **Channel** drop-down list.
2. Use the navigation keys to select a channel number. The default is **Channel 1 (2412 MHz)**.

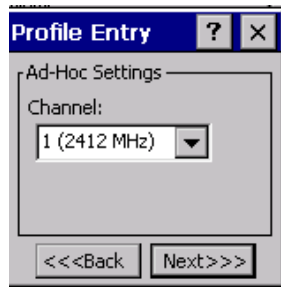


Figure 5-5 Ad-Hoc Settings Dialog Box

3. Press **TAB** twice to highlight the **Next** button.
4. Press **ENTER**. The **Encryption** dialog box displays. See [Encryption on page 5-15](#) for encryption options.

Authentication

Use the **Authentication** dialog box to configure authentication. If you selected **Ad-Hoc** mode, this dialog box is not available and authentication is set to **None** by default.

1. Use the navigation keys to select an authentication type from the drop-down list.
2. Press **TAB** twice to highlight the **Next** button.
3. Press **ENTER**.

Selecting **PEAP** or **TTLS** displays the **Tunneled** dialog box. Selecting **None**, **TLS**, or **LEAP** displays the **Encryption** dialog box. See [Encryption on page 5-15](#) for encryption options. [Table 5-6](#) lists the available authentication options.



Figure 5-6 Authentication Dialog Box

Table 5-6 Authentication Options

Authentication	Description
None	Default setting when authentication is not required on the network.
TLS (Fusion 2.4) EAP-TLS (Fusion 2.5)	Select this option to enable EAP-TLS authentication. EAP-TLS is an authentication scheme through IEEE 802.1x. It authenticates users and ensures only valid users can connect to the network. It also restricts unauthorized users from accessing transmitted information by using secure authentication certificates.
PEAP	Select this option to enable PEAP authentication. This method uses a digital certificate to verify and authenticate a user's identity.
LEAP	Select this option to enable LEAP authentication, which is based on mutual authentication. The AP and the connecting wearable terminal require authentication before gaining access to the network.
TTLS	Select this option to enable TTLS authentication.

Tunneled Authentication

Use the **Tunneled Authentication** dialog box to select the tunneled authentication options. There are different selections available for PEAP or TTLS authentication.

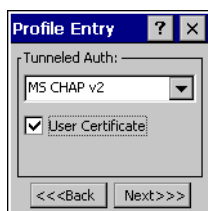


Figure 5-7 Tunneled Authentication Dialog Box

To select a tunneled authentication type:

1. Use the navigation keys to select a tunneled authentication type from the drop-down list. See [Table 5-7](#) and [Table 5-8](#).
If you selected the TLS tunnel type that requires a user certificate, the check box is already selected.
2. Press **TAB**.
3. Press **ALT > BKSP** (SPACE) to select the **User Certificate** check box if a certificate is required.
4. Press **TAB** to highlight the **Next** button.

5. Press **ENTER**. The **Installed User Certificates** dialog box appears.

[Table 5-7](#) lists the PEAP tunneled authentication options.

Table 5-7 PEAP Tunneled Authentication Options

PEAP Tunneled Authentication	Description
MS CHAP v2	Microsoft Challenge Handshake Authentication Protocol version 2 (MS CHAP v2) is a password-based, challenge-response, mutual authentication protocol that uses the industry-standard Message Digest 4 (MD4) and Data Encryption Standard (DES) algorithms to encrypt responses. The authenticating server challenges the access client and the access client challenges the authenticating server. If either challenge is not correctly answered, the connection is rejected. MS CHAP v2 was originally designed by Microsoft as a PPP authentication protocol to provide better protection for dial-up and virtual private network (VPN) connections. With Windows XP SP1, Windows XP SP2, Windows Server 2003, and Windows 2000 SP4, MS CHAP v2 is also an EAP type.
TLS	EAP TLS is used during phase 2 of the authentication process. This method uses a user certificate to authenticate.

[Table 5-8](#) lists the TTLS tunneled authentication options.

Table 5-8 TTLS Tunneled Authentication Options

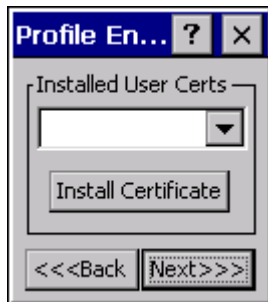
TTLS Tunneled Authentication	Description
CHAP	Challenge Handshake Authentication Protocol (CHAP) is one of the two main authentication protocols used to verify the user name and password for PPP Internet connections. CHAP is more secure than PAP because it performs a three way handshake during the initial link establishment between the home and remote machines. It can also repeat the authentication anytime after the link is established.
MS CHAP	Microsoft Challenge Handshake Authentication Protocol (MS CHAP) is an implementation of the CHAP protocol that Microsoft created to authenticate remote Windows workstations. MS CHAP is identical to CHAP, except that MS CHAP is based on the encryption and hashing algorithms used by Windows networks, and the MS CHAP response to a challenge is in a format optimized for compatibility with Windows operating systems.

Table 5-8 *TTLS Tunneled Authentication Options (Continued)*

TTLS Tunneled Authentication	Description
MS CHAP v2	MS CHAP v2 is a password based, challenge response, mutual authentication protocol that uses the industry standard Message Digest 4 (MD4) and Data Encryption Standard (DES) algorithms to encrypt responses. The authenticating server challenges the access client and the access client challenges the authenticating server. If either challenge is not correctly answered, the connection is rejected. MS CHAP v2 was originally designed by Microsoft as a PPP authentication protocol to provide better protection for dial-up and virtual private network (VPN) connections. With Windows XP SP1, Windows XP SP2, Windows Server 2003, and Windows 2000 SP4, MS CHAP v2 is also an EAP type.
PAP	Password Authentication Protocol (PAP) has two variations: PAP and CHAP PAP. It verifies a user name and password for PPP Internet connections, but it is not as secure as CHAP, since it works only to establish the initial link. PAP is also more vulnerable to attack because it sends authentication packets throughout the network. Nevertheless, PAP is more commonly used than CHAP to log in to a remote host like an Internet service provider.
MD5	Message Digest-5 (MD5) is an authentication algorithm developed by RSA. MD5 generates a 128-bit message digest using a 128-bit key, IPSec truncates the message digest to 96 bits.

User Certificate Selection

If you checked the **User Certificate** check box on the **Tunneled Authentication** dialog box or if **TLS** is the selected authentication type, the **Installed User Certificates** dialog box displays. Use the navigation keys to select a certificate from the drop-down list of currently installed certificates before proceeding. The selected certificate's name appears in the drop-down list. If the required certificate is not in the list, install it.

**Figure 5-8** *Installed User Certificates Dialog Box*

User Certificate Installation

To install a user certificate (EAP TLS only) and a server certificate for EAP TLS and PEAP authentication:

1. Press **TAB** to highlight the **Install Certificate** button.
2. Press **ENTER**. The **Credentials** dialog box appears.

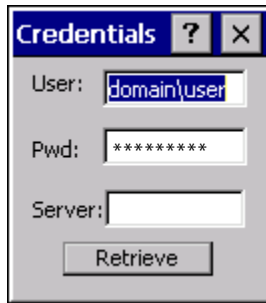


Figure 5-9 Credentials Dialog Box

3. Enter the **User:**, **Pwd:** (password), and **Server:** information in their respective text boxes. Press **TAB** to move to each field.
4. Press **TAB** to highlight the **Retrieve** button.
5. Press **ENTER**. A **Progress** dialog indicates the status of the certificate retrieval.
6. Press **ENTER** exit.

After the installation completes, the **Installed User Certs** dialog box displays and the certificate is available in the drop-down list for selection.

✓ **NOTE** To successfully install a user certificate, the wearable terminal must already be connected to a network from which the server is accessible.

Server Certificate Selection

If you select the **Validate Server Certificate** check box, a server certificate is required. Select a certificate on the **Installed Server Certificates** dialog box. An hour glass may appear as the wizard populates the existing certificate list. If the required certificate is not listed, install it:

1. Press **TAB** to highlight the **Install Certificate** button.
2. Press **ENTER**.

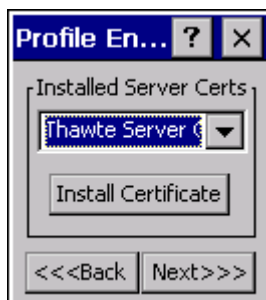


Figure 5-10 Installed Server Certificates Dialog Box

A dialog box appears that lists the currently loaded certificate files found in the default directory (Application) with the default extension.

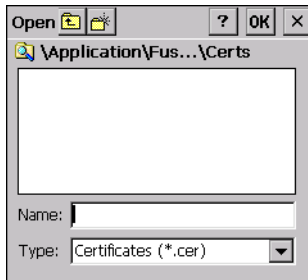


Figure 5-11 Browse Server Certificates

- a. Navigate to the folder where the certificate is stored. Select the certificate filename and then select **ok**.
3. A confirmation dialog verifies the installation. If the information in this dialog is correct, select the **Yes** button, If the information in this dialog is not correct select the **No** button. The wizard returns to the **Installed Server Certs** dialog box.

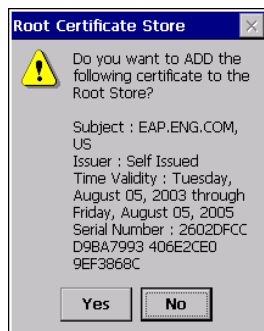


Figure 5-12 Confirmation Dialog Box

Credential Cache Options

If you selected any of the password-based authentication types, you can select different credential caching options. These options specify when the network credential prompts appear: at connection, on each resume, or at a specified time.

Entering the credentials directly into the profile permanently caches the credentials. In this case, the wearable terminal does not require user login. If a profile does not contain credentials entered through the configuration editor, you must log in to the wearable terminal before connecting.

Caching options only apply on credentials entered through the login dialog box.

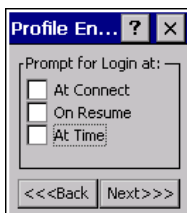


Figure 5-13 Prompt for Login at Dialog Box

If the wearable terminal does not have the credentials, you are prompted to enter a username and password. If the wearable terminal has the credentials (previous entered via a login dialog box), it uses these credentials unless the

caching options require the wearable terminal to prompt for new credentials. If you entered the credentials via the profile, the wearable terminal does not prompt for new credentials. [Table 4-9](#) lists the caching options.

Table 5-9 *Cache Options*

	Description
At Connect	Select this option to prompt for credentials whenever the wearable terminal tries to connect to a new profile. Deselect this to use the cached credentials to authenticate. If the credentials are not cached, you are prompted to enter credentials. This option only applies when logged in.
On Resume	Selecting this reauthenticates an authenticated user when a suspend/resume occurs. Once reauthenticated, the user is prompted for credentials. If the user does not enter the same credentials that were entered prior to the suspend/resume within three attempts, the user is disconnected from the network. This option only applies when logged in.
At Time	Select this option to perform a local verification on an authenticated user at a specified time. The time can be an absolute time or a relative time from the authentication, and should be in at least 5 minute intervals. Once the time has passed, the user is prompted for credentials. If the user does not enter the correct credentials within three attempts, the user is disconnected from the network. This option only applies when logged in.

Entering credentials applies these credentials to a particular profile. Logging out clears all cached credentials. Editing a profile clears all cached credentials for that profile.

The following authentication types have credential caching:

- EAP TLS
- PEAP
- LEAP
- TTLS.

Selecting the **At Time** check box displays the **Time Cache Options** dialog box.

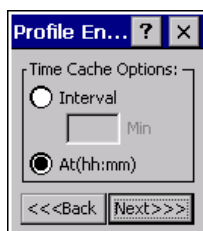


Figure 5-14 *Time Cache Options Dialog Box*

1. Select the **Interval** radio button to check credentials at a set time interval.
2. Enter the value in minutes in the **Min** box.
3. Select the **At (hh:mm)** radio button to check credentials at a set time.
4. Press **TAB** to highlight the **Next** button.
5. Press **ENTER**. The **At Time** dialog box appears.

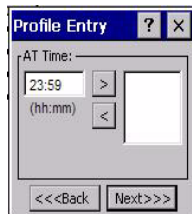


Figure 5-15 *At Time Dialog Box*

6. Enter the time using the 24 hour clock format in the **(hh:mm)** box.
7. Press **TAB** to highlight the > button.
8. Press **ENTER**. to move the time to the right text box. Repeat for additional time periods.
9. Press **TAB** to highlight the **Next** button. The **User Name** dialog box displays.

User Name

The user name and password can be entered (but is not required) when the profile is created. When a profile authenticates with credentials that were entered in the profile, caching rules do not apply. Caching rules only apply on credentials that are entered through the login dialog box.

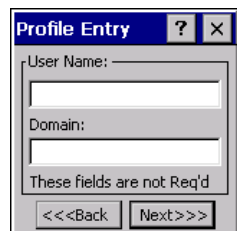


Figure 5-16 *Username Dialog Box*

1. Enter the username in the **User Name** text box.
2. Press **TAB**.
3. Enter the domain name in the **Domain** text box.
4. Press **TAB** twice to highlight the **Next** button.
5. Press **ENTER**. The **Password** dialog box appears.

Password

Use the **Password** dialog box to enter a password. If EAP/TLS is the selected authentication type, the password is not required and the field is disabled.



Figure 5-17 Password Dialog Box

1. Enter a password in the **Password** field.
2. Press **TAB** to highlight the **Advanced ID** check box.
3. Press **ALT > BKSP** (SPACE) to select the **Advanced ID** check box, if advanced identification is required.
4. Press **TAB** twice to highlight the **Next** button.
5. Press **ENTER**. The **Encryption** dialog box displays. See [Encryption on page 4-17](#).

Advanced Identity

Use the **Advanced ID** dialog box to enter the 802.1X identity to supply to the authenticator. This value can be 63 characters long and is case sensitive. In TTLS and PEAP, it is recommended entering the identity *anonymous* (rather than a true identity) plus any desired realm (e.g., anonymous@myrealm). A user ID is required before proceeding.

✓ **NOTE** When authenticating with a Microsoft IAS server, do not use advanced identity.

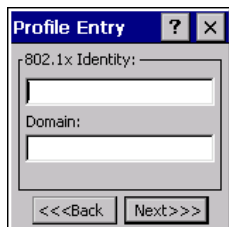


Figure 5-18 Advanced Identity Dialog Box

1. Enter the 802.1x identity information in the **802.1x Identity** field.
2. Press **TAB**.
3. Enter the domain name in the **Domain** field.
4. Press **TAB** twice to highlight the **Next** button.
5. Press **ENTER**. The **Encryption** dialog box displays.

Encryption

Use the **Encryption** dialog box to select an encryption type. The drop-down list includes encryption types available for the selected authentication type. See [Table 5-10](#) for these encryption types.

1. Use the navigation keys to select an encryption type.
 - If **40-Bit WEP** or **128-Bit WEP** are selected, the Key Index and Use Passkey fields appear.

2. Press **TAB**.
3. Use the navigation keys to select a key index number.
4. Press **TAB**.
5. Press **ALT > BKSP** (SPACE) to select the **Use Passkey** check box.
6. Press **TAB** twice to highlight the **Next** button.
7. Press **ENTER**.

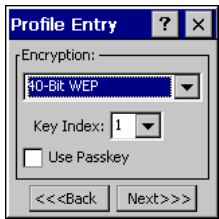


Figure 5-19 Encryption Dialog Box

Table 5-10 Encryption Options

Encryption	Description
Open	Select Open (the default) when no data packet encryption is needed over the network. Selecting this option provides no security for data transmitting over the network.
40-Bit WEP	<p>Select 40-Bit WEP to use 40-bit key length WEP encryption. WEP keys are manually entered in the edit boxes. Only the required number of edit boxes for a key length is displayed (10 Hex digit value for 40-bit keys). Use the Key Index drop-down list to configure the four WEP keys. The adapter uses the selected key. Note: The default Hex digit keys are visible any time they are used. As a security precaution after setting the key values for the network, the digits are replaced with asterisks * in the encryption key fields.</p> <p>If the associated AP uses an optional passkey, the active adapter WLAN profile must use one as well. The passkey is a plain text representation of the WEP keys displayed in the encryption dialog box. The passkey provides an easy way to enter WEP key data without having to remember the entire 40-bit (10 character) Hex digit string.</p>
128-Bit WEP	<p>Select 128-Bit WEP to use 128-bit key length WEP encryption. WEP keys are manually entered in the edit boxes. Only the required number of edit boxes for a key length is displayed (26 Hex digit value for 128-bit keys). Use the Key Index drop-down list to configure the four WEP keys. The adapter uses the selected key. Note: The default Hex digit keys are visible any time they are used. As a security precaution after setting the key values for the network, the digits are replaced with asterisks * in the encryption key fields.</p> <p>If the associated AP uses an optional passkey, the active adapter WLAN profile must use one as well. The passkey is a plain text representation of the WEP keys displayed in the encryption dialog box. The passkey provides an easy way to enter WEP key data without having to remember the entire 128-bit (26 character) Hex digit string.</p>
TKIP	Select this option to use Wireless Protected Access (WPA) via TKIP. Manually enter the shared keys in the passkey field. Select Next to display the passkey dialog box. Enter an 8 to 63 character string.
AES (Fusion 2.5 only)	Select this option to use Advanced Encryption Standard (AES). Manually enter the shared keys in the passkey field. Tap Next to display the passkey dialog box. Enter an 8 to 63 character string.

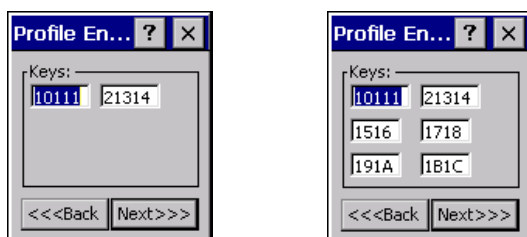
Table 5-11 Encryption / Authentication Matrix

Authentication	Encryption			
	Open	WEP	TKIP	AES (Fusion 2.5 only)
None	Yes	Yes	Yes	Yes
EAP TLS	No	Yes	Yes	Yes
PEAP	No	Yes	Yes	Yes
LEAP	No	Yes	Yes	Yes
TTLS	No	Yes	Yes	Yes

Key Entry Page

If you select either **40-Bit WEP** or **128-Bit WEP** the wizard proceeds to the key entry dialog box unless the **Use Passkey** check box was selected in the **Encryption** dialog box (see [Figure 4-21 on page 4-17](#)). The **Key Entry** dialog box will be shown only if the authentication is set to **None**. To enter the key information:

1. Enter the 40-bit or 128-bit keys into the fields. Press **TAB** to move to the next field.
2. Press **TAB** to highlight the **Next** button.
3. Press **ENTER**.



40-Bit WEP Keys Dialog Box 128-Bit WEP Keys Dialog Box

Figure 5-20 40-Bit and 128-Bit WEP Keys Dialog Boxes

Passkey Dialog

When you select **None** as an authentication and **WEP** as an encryption, you can choose to enter a passkey by checking the **Use PassKey** check box. The user is prompted to enter the passkey. For WEP, the **Use PassKey** checkbox is only available if the authentication is **None**.

When you select **None** as an authentication and **TKIP** as an encryption, you must enter a passkey. The user cannot enter a passkey if the encryption is **TKIP** and the authentication is anything other than **None**.

When you select **None** as an authentication and **AES** as an encryption, you must enter a passkey. The user cannot enter a passkey if the encryption is **AES** and the authentication is anything other than **None**.



Figure 5-21 Passkey Dialog Box

1. Enter the passkey in the **Passkey** text box.
2. Press **TAB** twice to highlight the **Next** button.
3. Press **ENTER**. The **IP Address Entry** dialog box displays.

IP Address Entry

Use the **IP Address Entry** dialog box to configure network address parameters: IP address, subnet, gateway, DNS, and WINS.

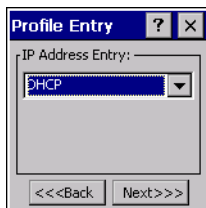


Figure 5-22 IP Address Entry Dialog Box

Table 5-12 IP Address Entry

Encryption	Description
DHCP	Select Dynamic Host Configuration Protocol (DHCP) from the IP Address Entry drop-down list to obtain a leased IP address and network configuration information from a remote server. DHCP is the default setting for the wearable terminal profile. When DHCP is selected, the IP address fields are read-only.
Static	Select Static to manually assign the IP, subnet mask, default gateway, DNS, and WINS addresses the wearable terminal profile uses.

1. Use the navigation keys to select either **DHCP** or **Static** from the drop-down list.
2. Press **TAB** twice to highlight the **Next** button.
3. Press **ENTER**.
 Selecting **Static IP** displays the **IP Address Entry** dialog box. Selecting **DHCP** displays the **Transmit Power** dialog box.

Use the **IP Address Entry** dialog box to enter the IP address and subnet information.

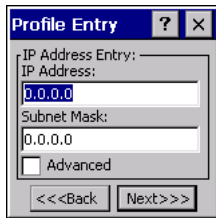


Figure 5-23 Static IP Address Entry Dialog Box

1. Enter the IP address in the **IP Address** text box.
2. Press **TAB**.
3. Enter the subnet mask address in the **Subnet Mask** text box.

Table 5-13 Static IP Address Entry Fields

Field	Description
IP Address	The Internet is a collection of networks with users that communicate with each other. Each communication carries the address of the source and destination networks and the particular machine within the network associated with the user or host computer at each end. This address is called the IP address (Internet Protocol address). Each node on the IP network must be assigned a unique IP address that is made up of a network identifier and a host identifier. Enter the IP address as a dotted-decimal notation with the decimal value of each octet separated by a period, for example, 192.168.7.27.
Subnet Mask	Most TCP/IP networks use subnets to manage routed IP addresses. Dividing an organization's network into subnets allows it to connect to the Internet with a single shared network address, for example, 255.255.255.0.

Select the **Advanced** check box, then select **NEXT** to display the **Advanced Address Entry** dialog box. Enter the Gateway, DNS, and WINS address. Select **NEXT** without selecting the **Advanced** check box to display the **Transmit Power** dialog box.

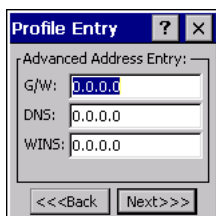


Figure 5-24 Advanced Address Entry Dialog Box

The IP information entered in the profile is only used if you selected the **Enable IP Mgmt** check box in the **Options > System Options** dialog box ([System Options on page 4-38](#)). If you didn't select this, the IP information in the profile is ignored and the IP information entered in the Microsoft interface applies.

Table 5-14 IP Config Advanced Address Entry Fields

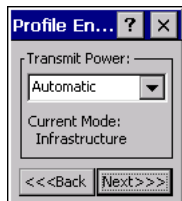
Field	Description
G/W	The default gateway forwards IP packets to and from a remote destination.
DNS	The Domain Name System (DNS) is a distributed Internet directory service. DNS translates domain names and IP addresses, and controls Internet email delivery. Most Internet services require DNS to operate properly. If DNS is not configured, Web sites cannot be located and/or email delivery fails.
WINS	WINS is a Microsoft® Net BIOS name server. WINS eliminates the broadcasts needed to resolve computer names to IP addresses by providing a cache or database of translations.

Select **Next**. The **Transmit Power** dialog box displays.

Transmit Power

The **Transmit Power** drop-down list contains different options for Ad-Hoc and Infrastructure mode. Automatic (i.e., use the current AP settings) and Power Plus (use higher than the current AP settings) are available for **Infrastructure** mode.

Adjusting the radio transmission power level enables the user to expand or confine the transmission area with respect to other wireless devices that could be operating nearby. Reducing coverage in high traffic areas improves transmission quality by reducing the amount of interference in that coverage area.

**Figure 5-25** Transmit Power Dialog Box (Infrastructure Mode)**Table 5-15** Transmit Power Dialog Box (Infrastructure Mode)

Field	Description
Automatic	Select Automatic (the default) to use the AP power level.
Power Plus	Select Power Plus to set the wearable terminal transmission power one level higher than the level set for the AP.

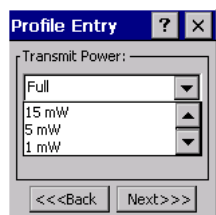


Figure 5-26 Transmit Power Dialog Box (Ad-Hoc Mode)

Table 5-16 Power Transmit Options (Ad-Hoc Mode)

Field	Description
Full	Select Full power for the highest transmission power level. Select Full power when operating in highly reflective environments and areas where other devices could be operating nearby, or when attempting to communicate with devices at the outer edge of a coverage area.
30 mW	Select 30 mW to set the transmit power level to 30 mW.
15 mW	Select 15 mW to set the transmit power level to 15 mW.
5 mW	Select 5 mW to set the transmit power level to 5 mW.
1 mW	Select 1 mW for the lowest transmission power level. Use this level when communicating with other devices in very close proximity, or in instances where you expect little or no radio interference from other devices.

Select **Next** to display the **Battery Usage** dialog box.

Battery Usage

Use the **Battery Usage** dialog box to select power consumption of the wireless LAN. There are three settings available: **CAM**, **Fast Power Save**, and **MAX Power Save**. Battery usage cannot be configured in Ad-Hoc profiles.

Use the navigation keys to select an entry. Press **TAB** twice to highlight **Finish**.

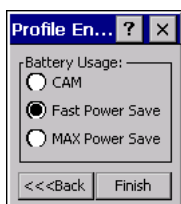


Figure 5-27 Battery Usage Dialog Box



NOTE Power consumption is also related to the transmit power settings.

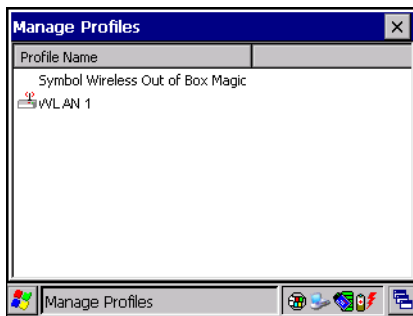
Table 5-17 Battery Usage Options

Field	Description
CAM	Continuous Aware Mode (CAM) provides the best network performance, but yields the shortest battery life.
Fast Power Save	Fast Power Save (the default) performs in the middle of CAM and MAX Power Save with respect to network performance and battery life.
MAX Power Save	Max Power Save yields the longest battery life while potentially reducing network performance. In networks with minimal latency, Max Power Save performs as well as Fast Power Save, but with increased battery conservation.

Manage Profiles Application

The **Manage Profiles** window provides a list of user-configured wireless profiles. Define up to 32 profiles at any one time. To open the **Manage Profiles** window:

1. Press **ALT - w**. The Wireless menu appears.
2. Using the navigation keys, select the **Manage Profiles**.
3. Press **ENTER** key. The **Manage Profiles** window displays.

**Figure 5-28** Manage Profiles Window

Icons next to each profile identify the profile's current state.

Table 5-18 Profile Icons








Icon	Description
No Icon	Profile is not selected, but enabled.
	Profile is disabled.
	Profile is cancelled. A cancelled profile is disabled until a connect or login function is performed through the configuration editor.
	Profile is in use and describes an infrastructure profile not using encryption.
	Profile is in use and describes an infrastructure profile using encryption.

Table 5-18 Profile Icons (Continued)

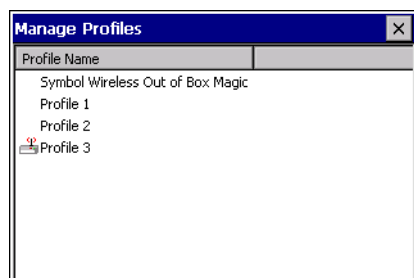
Icon	Description
	Profile is in use and describes an ad-hoc profile not using encryption.
	Profile is in use and describes an ad-hoc profile using encryption.
	Profile is not valid in the device current operating regulatory domain.

The profiles are listed in priority order for use by the automatic roaming feature. Change the order by moving profiles up or down. To edit existing profiles, use the navigation keys to select a profile, press **ALT - m** and select an option from the menu to connect, edit, disable (enable), or delete the profile. (Note that the **Disable** menu item changes to **Enable** if the profile is already disabled.)

**Figure 5-29** Manage Profiles Context Menu

Changing Profiles

A completed profile is a set of configuration settings that can be used in different locations to connect to a wireless network. Create different profiles to have pre-defined operating parameters available for use in various network environments. When the **WLAN Profiles** window displays, existing profiles appear in the list.

**Figure 5-30** Manage Profiles

Use the navigation keys to select a profile and press **Blue key - TAB (Menu)** to open the pop-up menu. Select **Connect** and then press **ENTER** to set this as the active profile. Once selected, the wearable terminal uses the authentication, encryption, ESSID, IP Config, and power consumption settings configured for that profile.

Editing a Profile

Use the navigation keys to select a profile and press **Blue key - TAB (Menu)** to open the pop-up menu. Select **Edit** and then press **ENTER** to display the **Profile Wizard** where you can set the ESSID and operating mode for the

profile. Use the **Profile Wizard** to edit the profile power consumption and security parameters. See [Profile Editor Wizard on page 4-6](#).

Creating a New Profile

To create new profiles from the **Manage Profiles** window, press **Blue key - TAB (Menu)**.

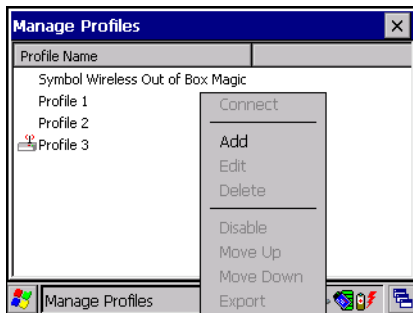


Figure 5-31 *Manage Profiles - Add*

Select **Add** and press **ENTER** to display the **Profile Wizard** wherein you can set the profile name and ESSID. Set security, network address information, and power consumption level for the new profile.

Deleting a Profile

To delete a profile from the list, use the navigation keys to select a profile and then press **Blue key - TAB (Menu)** to open the pop-up menu. Select **Delete** and then press **ENTER**. A confirmation dialog box appears.

Ordering Profiles

To order the profile, select a profile using the navigation keys and press **Blue key - TAB (Menu)** to open the pop-up menu. Select **Move Up** or **Move Down** from the pop-up menu and press **ENTER**. If the current profile association is lost, the wearable terminal attempts to associate with the first profile in the list, then the next, until it achieves a new association.

✓ **NOTE** Profile Roaming must be enabled.

Export a Profile

To export a profile to a registry file, select a profile using the navigation keys and press **Blue key - TAB (Menu)**. Select **Export** from the pop-up menu and press **ENTER**. The **Save As** dialog box displays with the **Application** folder and a default name of `WCS_PROFILE{profile GUID}.reg` (Globally Unique Identifier).

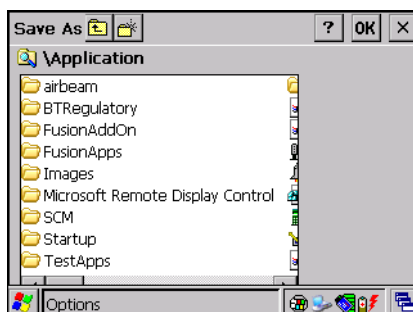


Figure 5-32 *Save As Dialog Box*

If required, change the name in the **Name** field and select **Save**. A confirmation dialog box appears after the export completes.

Wireless Status Application

To open the **Wireless Status** window, press **ALT - w**, select **Wireless Status** and press **ENTER**. The **Wireless Status** window displays information about the wireless connection.

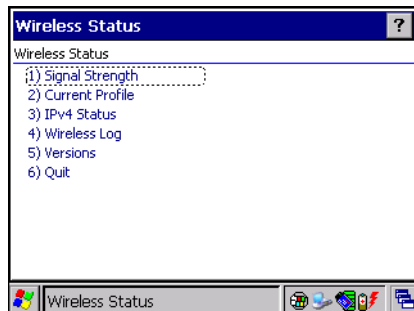


Figure 5-33 *Wireless Status Window*

The **Wireless Status** window contains the following options. Select the option to display the option window.

- Signal Strength - provides information about the connection status of the current wireless profile.
- Current Profile - displays basic information about the current profile and connection settings.
- IPv4 Status - displays the current IP address, subnet, and other IP related information assigned to the wearable terminal.
- Wireless Log - displays a log of important recent activity, such as authentication, association, and DHCP renewal completion, in time order.
- Versions - displays software, firmware, and hardware version numbers.
- Quit - exits the **Wireless Status** window.

Signal Strength Window

The **Signal Strength** window provides information about the connection status of the current wireless profile including signal quality, missed beacons, and transmit retry statistics. The BSSID address (shown as *AP MAC Address*) displays the AP currently associated with the connection. In Ad-Hoc mode, the AP MAC Address shows the BSSID of the Ad-Hoc network. Information in this window updates every 2 seconds.

To open the **Signal Status** window, press **1**.

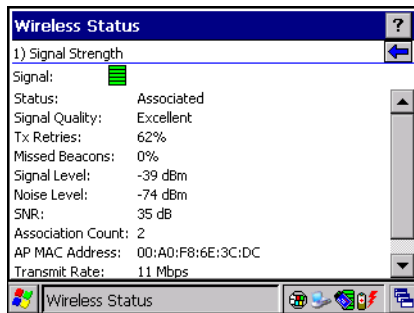


Figure 5-34 Signal Strength Window

After viewing the **Signal Strength** window, press **ESC** to return to the **Wireless Status** window.

Table 5-19 Signal Strength Status

Field	Description
Signal	Displays the Relative Signal Strength Indicator (RSSI) of the signal transmitted between the AP and wearable terminal. As long as the Signal Quality icon is green the AP association is not jeopardized. If the icon is red (poor signal), an association with a different AP could be warranted to improve the signal. The signal strength icon changes depending on the signal strength.
	Excellent Signal
	Very Good Signal
	Good Signal
	Fair Signal
	Poor Signal
	Out of Range (no signal)
	The radio card is off or there is a problem communicating with the radio card.
Status	Indicates if the wearable terminal is associated with the AP.
Signal Quality	Displays a text format of the Signal icon.
Tx Retries	Displays a percentage of the number of data packets the wearable terminal retransmits. The fewer transmit retries, the more efficient the wireless network is.
Missed Beacons	Displays a percentage of the amount of beacons the wearable terminal missed. The fewer transmit retries, the more efficient the wireless network is. Beacons are uniform system packets broadcast by the AP to keep the network synchronized.
Signal Level	Displays the AP signal level in decibels per milliwatt (dBm).
Noise Level	Displays the background interference (noise) level in decibels per milliwatt (dBm).
SNR	Displays the access point/wearable terminal Signal to Noise Ratio (SNR) of signal strength to noise (interference) in decibels per milliwatt (dBm).

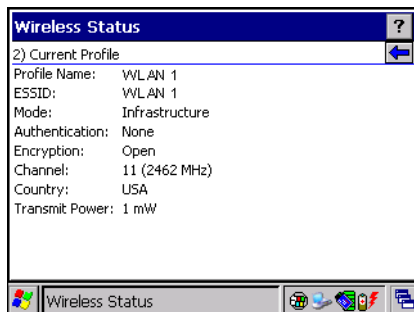
Table 5-19 *Signal Strength Status (Continued)*

Field	Description
Association Count	Displays the number of APs the wearable terminal connects to while roaming.
AP MAC Address	Displays the MAC address of the AP to which the wearable terminal is connected.
Transmit Rate	Displays the current rate of the data transmission.

Current Profile Window

The **Current Profile** window displays basic information about the current profile and connection settings. This window updates every two seconds.

To open the **Current Profile** window, press **2**.

**Figure 5-35** *Current Profile Window***Table 5-20** *Current Profile Window*

Field	Description
Profile Name	Displays the current profile name the wearable terminal uses to communicate with the AP.
ESSID	Displays the current profile ESSID name.
Mode	Displays the current profile mode, either Infrastructure or Ad-Hoc.
Authentication	Displays the current profile's authentication type.
Encryption	Displays the current profile's encryption type.
Channel	Displays the current profile's channel setting.
Country	Displays the current profile's country setting.
Transmit Power	Displays the radio transmission power level.

IPv4 Status Window

The **IPv4 Status** window displays the current IP address, subnet, and other IP related information assigned to the wearable terminal. It also allows renewing the address if the profile is using DHCP to obtain the IP information. Select **Renew** to initiate a full DHCP discover. The **IPv4 Status** window updates automatically when the IP address changes.

To open the **IPv4 Status** window, press **3**.

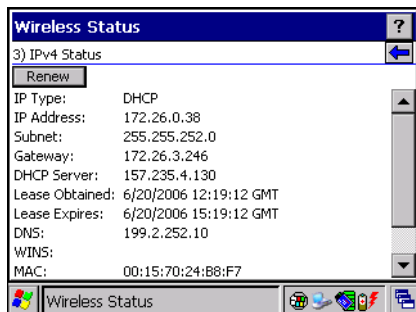


Figure 5-36 IPv4 Status Window

Table 5-21 IPv4 Status Fields

Field	Description
IP Type	Displays the IP type for the current profile: DHCP or Static . If the IP type is DHCP, leased IP address and network address data appear for the wearable terminal. If the IP type is Static, the values displayed were input manually in the IP Config tab on page 4-19 .
IP Address	Displays the wearable terminal's IP address. The Internet is a collection of networks with users that communicate with each other. Each communication carries the address of the source and destination networks and the particular machine within the network associated with the user or host computer at each end. This address is called the IP address. Each node on the IP network must be assigned a unique IP address that is made up of a network identifier and a host identifier. The IP address as a dotted-decimal notation with the decimal value of each octet separated by a period, for example, 192.168.7.27.
Subnet	Displays the subnet address. Most TCP/IP networks use subnets to manage routed IP addresses. Dividing an organization's network into subnets allows it to connect to the Internet with a single shared network address, for example, 255.255.255.0.
Gateway	Displays the gateway address. A gateway forwards IP packets to and from a remote destination.
DCHP Server	The Domain Name System (DNS) is a distributed Internet directory service. DNS translates domain names and IP addresses, and controls Internet e-mail delivery. Most Internet services require DNS to operate properly. If DNS is not configured, Web sites cannot be located or e-mail delivery fails.
Lease Obtained	Displays the date that the IP address was obtained.
Lease Expires	Displays the date that the IP address expires and a new IP address is requested.
DNS	Displays the IP address of the DNS server.
WINS	WINS is a Microsoft Net BIOS name server. WINS eliminates the broadcasts needed to resolve computer names to IP addresses by providing a cache or database of translations.
MAC	An IEEE 48-bit address is assigned to the wearable terminal at the factory to uniquely identify the adapter at the physical layer.
Host Name	Displays the name of the wearable terminal.

Wireless Log Window

The **Wireless Log** window displays a log of recent activity, such as authentication, association, and DHCP renewal completion, in time order. Save the log to a file or clear the log (within this instance of the application only). The auto-scroll feature automatically scrolls down when new items are added to the log.

To open the **Wireless Log** window, press **4**. The **Wireless Log** window displays.



Figure 5-37 *Wireless Log Window*

Saving a Log

To save a Wireless Log:

1. Press **TAB** until the **Save** button is highlighted.
2. Press **Blue - BKSP**. The **Save As** dialog box displays.
3. Navigate to the desired folder.
4. In the **Name** field, enter a file name and then select **OK**. A text file is saved in the selected folder.

Clearing the Log

To clear the log, press **TAB** until the **Clear** button is highlighted. Press **Blue - BKSP**. The log clears.

Versions Window

The **Versions** window displays software, firmware, and hardware version numbers. This window only updates when it is displayed. There is no need to update constantly. The content of the window is determined at runtime, along with the actual hardware and software to display in the list. Executable paths of the software components on the list are defined in registry, so that the application can retrieve version information from the executable. "File not found" appears if the executable cannot be found at the specified path.

To open the **Versions** window, press **5**.

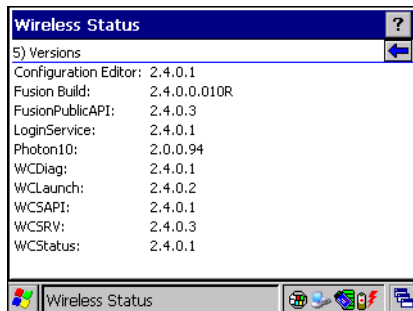


Figure 5-38 *Versions Window*

The window displays software version numbers for the following:

- Configuration Editor (Fusion 2.4 only)
- Fusion Build
- Public API
- LoginService
- Photon10
- WCCConfigEd (Fusion 2.5 only)
- WCDiag
- WCLaunch
- WCSAPI
- WCSRVR
- WCStatus.

Press **ESC** to return to the **Wireless Status** window.

Wireless Diagnostics Application

The **Wireless Diagnostics** application window provides links to perform ICMP Ping, Trace Routing, and Known APs. To open the **Wireless Diagnostics** window, press **ALT - w**, select **Wireless Diagnostics** using the navigation keys and press **ENTER**.

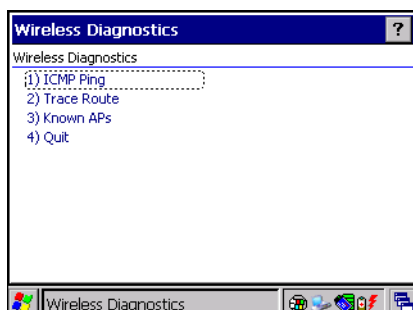


Figure 5-39 *Wireless Diagnostics Window*

The **Wireless Diagnostics** window contains the following options. Select the option to display the option window.

- ICMP Ping - tests the wireless network connection.
- Trace Route - tests a connection at the network layer between the wearable terminal and any place on the network.
- Known APs - displays the APs in range using the same ESSID as the wearable terminal.
- Quit - Exits the **Wireless Diagnostics** window.

To return to the **Wireless Diagnostics** window from an option window, press **ESC**.

ICMP Ping Window

The **ICMP Ping** window allows testing a connection at the network layer (part of the IP protocol) between the wearable terminal and an AP. Ping tests only stop when you select the **Stop Test** button, close the **Wireless Diagnostics** application, or if the wearable terminal switches between infrastructure and ad-hoc modes.

To open the **ICMP Ping** window, press **1**.

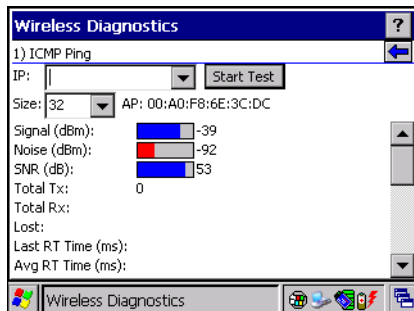


Figure 5-40 ICMP Ping Window

To perform an ICMP ping:

1. In the **IP** field, enter an IP address or select an IP address from the drop-down list.
2. Press **TAB** to highlight the **Size** drop-down list.
3. Using the navigation keys, select a size value.
4. Press **TAB** to highlight **Start Test**.
5. Press **Blue - BKSP (SPACE)**. The ICMP Ping test starts. Information of the ping test displays in the appropriate fields.

Trace Route Window

Trace Route traces a packet from a computer to a host, showing how many hops the packet requires to reach the host and how long each hop takes. The **Trace Route** utility identifies where the longest delays occur.

The **Trace Route** window allows testing a connection at the network layer (part of the IP protocol) between the wearable terminal and any place on the network.

To open the **Trace Route** window, press **2**.

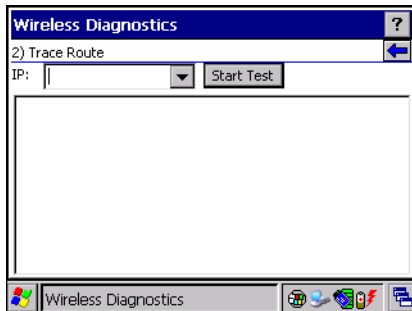


Figure 5-41 Trace Route Window

Enter an IP address or a DNS Name in the **IP** combo box. Press **TAB** to highlight **Start Test**. Press **Blue - BKSP**. The IP combo box should match the information shown in the **ICMP Ping** window's IP combo box. When starting a test, the trace route attempts to find all routers between the wearable terminal and the destination. The Round Trip Time (RTT) between the wearable terminal and each router appears, along with the total test time. The total test time may be longer than all RTTs added together because it does not only include time on the network.

Known APs Window

The **Known APs** window displays the APs in range using the same ESSID as the wearable terminal. This window is only available in **Infrastructure** mode. To open the **Known APs** window, press **3**.

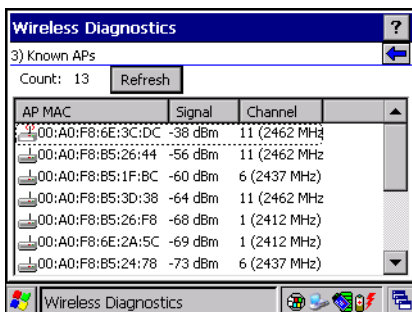






Figure 5-42 Known APs Window

See [Table 5-22](#) for the definitions of the icons next to the AP.

Table 5-22 Current Profile Window

Icon	Description
	Indicates that the AP is the associated access point, and is set to mandatory.
	Indicates that the AP is the associated access point, but is not set to mandatory.
	Indicates that the wearable terminal is not associated to this AP, but the AP is set as mandatory.
	Indicates that the wearable terminal is not associated to this AP, and AP is not set as mandatory.

Using the navigation keys select an AP. Press **Blue key - TAB (Menu)** to display a pop-up menu with the following options: **Set Mandatory** and **Set Roaming**.

Select **Set Mandatory** to prohibit the wearable terminal from associating with a different AP. The letter **M** displays on top of the icon. The wearable terminal connects to the selected AP and never roams until:

- You select **Set Roaming**

- The wearable terminal roams to a new profile
- The wearable terminal suspends
- The wearable terminal resets (warm or cold).

Select **Set Roaming** to allow the wearable terminal to roam to any AP with a better signal. These settings are temporary and never saved to the registry.

Select **Refresh** to update the list of the APs with the same ESSID. The highest signal strength value is 32.

Options

Use the wireless **Option** dialog box to select one of the following operation options from the drop-down list:

- Operating Mode Filtering
- Regulatory
- Band Selection
- System Options
- Change Password
- Export.

To open the **Options** window, press **ALT - w**, select **Options** using the navigation keys and press **ENTER**.

Operating Mode Filtering

The **Operating Mode Filtering** options cause the Find WLANs application to filter the available networks found.

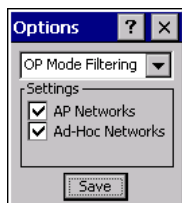


Figure 5-43 *OP Mode Filtering Dialog Box*

The **AP Networks** and **Ad-Hoc Networks** check boxes are selected by default. To select/de-select the checkboxes, press **TAB** to highlight a checkbox. Press **Blue - BKSP** to select or de-select the checkbox.

Table 5-23 *OP Mode Filtering Options*

Field	Description
AP Networks	Select the AP Networks check box to display available AP networks and their signal strength within the Available WLAN Networks (see Find WLANs Application on page 4-5). These are the APs available to the wearable terminal profile for association. If this option was previously disabled, refresh the Available WLAN Networks window to display the AP networks available to the wearable terminal.
AD-Hoc Networks	Select the Ad-Hoc Networks check box to display available peer (adapter) networks and their signal strength within the Available WLAN Networks . These are peer networks available to the wearable terminal profile for association. If this option was previously disabled, refresh the Available WLAN Networks window to display the Ad Hoc networks available to the wearable terminal.

Press **TAB** to highlight **Save** and then press **ENTER** to save the settings or press **ESC** to discard any changes. Press **ESC** to exit the **Options** dialog box.

Regulatory Options

Use the **Regulatory** settings to configure the country the wearable terminal is in. Due to regulatory requirements (within a country) a wearable terminal is only allowed to use certain channels.



Figure 5-44 *Regulatory Options Dialog Box*

Table 5-24 *Regulatory Options*

Field	Description
Settings	Select the country from the drop-down list. To connect to a profile, the profile country must match this setting, or the AP country setting if you select the Enable 802.11d check box.
Enable 802.11d	If you enable this setting the WLAN adapter attempts to retrieve the country setting from the APs. Profiles which use <i>Infrastructure</i> mode can only connect if this country setting is the same as the AP country setting or if the profile country setting is set to Allow Any Country . All APs must be configured to transmit the country information.

1. Press **TAB** to highlight the **Settings** drop-down menu. Use the scroll keys to select a country from the list.
2. Press **TAB** to highlight the **Enable 802.11d** checkbox. Press **Blue - BKSP** to enable or disable the check box.
3. Press **TAB** to highlight **Save** and then press **ENTER** to save the settings or press **ESC** to discard any changes.
4. Press **ESC** to exit the **Options** dialog box.

Band Selection

The **Band Selection** settings identify the frequency bands to scan when finding WLANs. These values refer to the 802.11 standard networks.

✓ **NOTE** Select one band for faster access when scanning for WLANs.



Figure 5-45 Band Selection Dialog Box

Table 5-25 Band Selection Options

Field	Description
2.4GHz Band	The Find WLANs application list includes all networks found in the 2.4 GHz band (802.11b and 802.11g).
5GHz Band	The Find WLANs application list includes all networks found in the 5 GHz band (802.11a).

1. Press **TAB** to highlight the **2.4 GHz Band** check box. Press **Blue - BKSP** to enable or disable the check box.
2. Press **TAB** to highlight the **5 GHz Band** check box. Press **Blue - BKSP** to enable or disable the check box.
3. Press **TAB** to highlight **Save** and then press **ENTER** to save the settings or press **ESC** to discard any changes.
4. Press **ESC** to exit the **Options** dialog box.

System Options

Use **System Options** to set miscellaneous system setting.



Figure 5-46 System Options Dialog Box

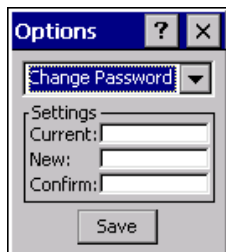
Table 5-26 System Options

Field	Description
Profile Roaming	Configures the wearable terminal to roam to the next available WLAN profile when it moves out of range of the current WLAN profile.
Enable IP Mgmt	Enables the Wireless Companion Services to handle IP address management. The Wireless Companion Service configures the IP based on what is configured in the network profile. Deselect this to manually configure the IP in the standard Windows IP window. Enabled by default.
Auto Time Config	Enables automatic update of the system time. Network association updates the device time based on the time set in the AP. This proprietary feature is only supported with Zebra infrastructure. Enabled by default.

1. Press **TAB** to highlight the **Profile Roaming** check box. Press **Blue - BKSP** to enable or disable the check box.
2. Press **TAB** to highlight the **Enable IP Mgmt** check box. Press **Blue - BKSP** to enable or disable the check box.
3. Press **TAB** to highlight the **Auto Time Config** check box. Press **Blue - BKSP** to enable or disable the check box.
4. Press **TAB** to highlight **Save** and then press **ENTER** to save the settings or press **ESC** to discard any changes.
5. Press **ESC** to exit the **Options** dialog box.

Change Password

Use **Change Password** to require a password before editing a profile. This allows pre-configuring profiles and prevents users from changing the network settings. The user can use this feature to protect settings from a guest user. By default, the password is not set.

**Figure 5-47** Change Password Window

To create a password for the first time, enter the new password in the **New:** and **Confirm:** text boxes. Select **Save**. The **Current:** text box does not appear if a password was not previously set.

To change an existing password, enter the current password in the **Current:** text box and enter the new password in the **New:** and **Confirm:** text boxes. Select **Save**.

To delete the password, enter the current password in the **Current:** text box and leave the **New:** and **Confirm:** text boxes empty. Select **Save**.



NOTE Passwords are case sensitive and can not exceed 160 characters.

Export

- ✓ **NOTE** Exporting options enables settings to persist after cold boot.

Use **Export** to export all profiles to a registry file, and to export the options to a registry file.



Figure 5-48 Options - Export Dialog Box

To export options:

1. Select **Export Options** and press **Blue - BKSP**. The **Save As** dialog box displays.

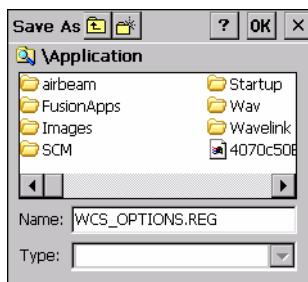


Figure 5-49 Export Options Save As Dialog Box

2. Enter a filename in the **Name:** field. The default filename is `WCS_OPTIONS.REG`.
3. Select **Save** and press **ALT- BKSP**.

To export all profiles:

1. Select **Export All Profiles** and press **ALT- BKSP**. The **Save As** dialog box displays.

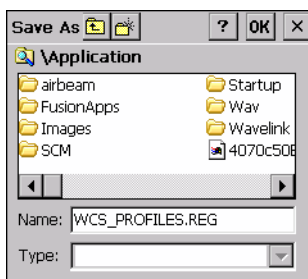


Figure 5-50 Export All Profiles Save As Dialog Box

2. Enter a filename in the **Name:** field. The default filename is `WCS_PROFILES.REG`.
3. In the **Folder:** drop-down list, select the desired folder.
4. Select **Save** and press **ALT- BKSP**.

Selecting **Export All Profiles** saves the current profile. This information is used to determine which profile to connect with after a warm boot or cold boot.

Persistence

Export options and profiles to provide cold boot persistence for Windows CE 5.0 devices. Save the exported registry files in the **Application** folder to use them on a cold boot or clean boot and restore previous profile and option settings.

Currently, only server certificates can be saved for persistence. To save server certificates for persistence, save the certificate files in the folder **Application** to install the certificates automatically on a cold or clean boot.

✓ **NOTE** User certificates cannot be saved for cold boot or clean boot persistence at this time.

Registry Settings

Use a registry key to modify some of the parameters. The registry path is:

HKLM\SOFTWARE\Symbol Technologies, Inc.\Configuration Editor

Table 5-27 Registry Parameter Settings

Key	Type	Default	Description												
CertificateDirectory	REG_SZ	\\Application	The default directory to find certificates.												
EncryptionMask	REG_DWORD	0x0000001F	<p>Defines the supported encryption types. This is a bitwise mask with each bit corresponding to an encryption type.</p> <p>1 = Type is supported 0 = Type is not supported</p> <table> <thead> <tr> <th>Bit Number</th> <th>Encryption Type</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>None</td> </tr> <tr> <td>1</td> <td>40-Bit WEP</td> </tr> <tr> <td>2</td> <td>128-Bit WEP</td> </tr> <tr> <td>3</td> <td>TKIP</td> </tr> <tr> <td>4</td> <td>AES (Fusion 2.5 only)</td> </tr> </tbody> </table>	Bit Number	Encryption Type	0	None	1	40-Bit WEP	2	128-Bit WEP	3	TKIP	4	AES (Fusion 2.5 only)
Bit Number	Encryption Type														
0	None														
1	40-Bit WEP														
2	128-Bit WEP														
3	TKIP														
4	AES (Fusion 2.5 only)														

Log On/Off Application

When the user launches the **Log On/Off** application, the wearable terminal may be in two states; the user may be logged onto the wearable terminal by already entering credentials through the login box, or there are no user logged on. Each of these states have a separate set of use cases and a different look to the dialog box.

User Already Logged In

If already logged into the wearable terminal, the user can launch the login dialog box for the following reasons:

- Connect to and re-enable a cancelled profile. To do this:
 - Launch the Log On/Off dialog.
 - Select the cancelled profile from the profile list.
 - Login to the profile.
- ✓ **NOTE** Re-enable cancelled profiles using the Profile Editor Wizard and choosing to connect to the cancelled profile. Cancelled profiles are also re-enabled when a new user logs on.
- Log off the wearable terminal to prevent another user from accessing the current users network privileges.
- Switch wearable terminal users to quickly logoff the wearable terminal and allow another user to log into the wearable terminal.

No User Logged In

If no user is logged into the wearable terminal, launch the login dialog box and log in to access user profiles.

The **Login** dialog box varies if it is:

- Launched by WCS, because the service is connecting to a new profile that needs credentials.
- Launched by WCS, because the service is trying to verify the credentials due to credential caching rules.
- Launched by a user, when a user is logged in.
- Launched by a user, when no user is logged in.

Table 5-28 *Log On/Off Options*

Field	Description
Wireless Profile Field	When launching the login application, the Wireless Profile field has available all the wireless profiles that require credentials. This includes profiles that use EAP TLS, PEAP, LEAP, and EAP-TTLS.
Profile Status Icon	The profile status icon (next to the profile name) shows one of the following states: The selected profile is cancelled. The selected profile is enabled but is not the current profile. The profile is the current profile (always the case for WCS Launched).

Table 5-28 *Log On/Off Options (Continued)*

Field	Description
Network Username and Password Fields	The Network Username and Network Password fields are used as credentials for the profile selected in the Wireless Profile field. Currently these fields are limited to 159 characters.
Mask Password Checkbox	The Mask Password checkbox determines whether the password field is masked (i.e., displays only the '*' character) or unmasked (i.e., displays the entered text). Check the box to unmask the password. Uncheck the box to mask the password (the default).
Status Field	The status field displays status that is important to the login dialog. If the user opens the dialog and needs to prompt for credentials for a particular profile at this time, it can use the status field to let the user know that the network is held up by the password dialog being open.

Selecting **OK** sends the credentials through WCS API. If there are no credentials entered, a dialog box displays informing the user which field was not entered.

The **Log Off** button only displays when a user is already logged on. When the **Log Off** button is selected, the user is prompted with three options: **Log Off**, **Switch Users**, and **Cancel**. Switching users logs off the current user and re-initialize the login dialog box to be displayed for when there is no user logged on. Logging off logs off the current user and close the login dialog box. **Cancel** closes the Log Off dialog box and the Login dialog box displays.

When the user is logged off, the wearable terminal only roams to profiles that do not require credentials or to profiles that were created with the credentials entered into the profile.

The **Cancel** button closes the dialog without logging into the network. If the login dialog was launched by the WCS and not by the user, selecting **Cancel** first causes a message box to display a warning that the cancel disables the current profile. If the user still chooses to cancel the login at this point, the profile is cancelled.

Once a profile is cancelled, the profile is terminal until a user actively re-enables it or a new user logs onto the wearable terminal.

Chapter 6 Using Bluetooth

Introduction



NOTE The VOWT4090 requires the use of a Remote Desktop software to configure settings and software. See for information on setting up the device with remote desktop software.

Bluetooth-equipped devices can communicate without wires, using frequency-hopping spread spectrum (FHSS) RF to transmit and receive data in the 2.4 GHz Industry Scientific and Medical (ISM) band (802.15.1). Bluetooth wireless technology is specifically designed for short-range (30 feet/10 meters) communications and low power consumption.

Wearable terminals with Bluetooth capabilities can exchange information (e.g., files, appointments and tasks) with other Bluetooth enabled devices such as headsets, printers, access points and other wearable terminals.

Zebra wearable terminals with Bluetooth technology use the StoneStreet One Bluetooth stack. To program Bluetooth within the wearable terminal refer to the StoneStreet One SDK, available at the Zebra Support Central web site. on the WT4000 product page.

Adaptive Frequency Hopping

Adaptive Frequency Hopping (AFH) is a method of avoiding fixed frequency interferers. AFH can be used with Bluetooth voice. All devices in the piconet (Bluetooth network) must be AFH-capable in order for AFH to work. There is no AFH when connecting and discovering devices. Avoid making Bluetooth connections and discoveries during critical 802.11b communications. AFH for Bluetooth can be broken-down into four main sections:

- Channel Classification - A method of detecting an interference on a channel-by-channel basis, or pre-defined channel mask.
- Link Management - Coordinates and distributes the AFH information to the rest of the Bluetooth network.
- Hop Sequence Modification - Avoids the interference by selectively reducing the number of hopping channels.
- Channel Maintenance - A method for periodically re-evaluating the channels.

When AFH is enabled, the Bluetooth radio “hops-around” (instead of through) the 802.11b high-rate channels. AFH coexistence allows Zebra wearable terminals to operate in any infrastructure. AFH is always enabled in the WT4090.

The Bluetooth radio in this wearable terminal operates as a Class 2 device power class. The maximum output power is 2.5mW and the expected range is up to 32.8 feet (10 meters). A definitive definition of ranges based on power class is difficult to obtain due to power and device differences, and whether one measures open space or closed office space.



NOTE It is not recommended to perform Bluetooth wireless technology inquiry when high rate 802.11b operation is required.

Security

The current Bluetooth specification defines security at the link level. Application-level security is not specified. This allows application developers to define security mechanisms tailored to their specific need. Link-level security is really between devices not users, while application-level security can be implemented on a per-user basis. The Bluetooth specification defines security algorithms and procedures needed to authenticate devices, and if needed, encrypt the data flowing on the link between the devices. Device authentication is a mandatory feature of Bluetooth while link encryption is optional.

Pairing of Bluetooth devices is accomplished by creating an initialization key that is used to authenticate the devices and create a link key for them. Entering a common PIN number in the devices being paired generates the initialization key. The PIN number is never sent over the air. By default, the Bluetooth stack responds with no key when a key is requested (it is up to user to respond to the key request event). Authentication of Bluetooth devices is based-upon a challenge-response transaction. Bluetooth allows for a PIN number or passkey that is used to create other 128-bit keys used for security and encryption. The encryption key is derived from the link key used to authenticate the pairing devices. Also worthy of note is the limited range and fast frequency hopping of the Bluetooth radios that makes long-distance eavesdropping difficult.

It is recommended:

- Perform pairing in a secure environment
- Keep PIN codes private and don't store the PIN codes in the wearable terminal
- Implement application-level security.

Turning the Bluetooth Radio Mode On and Off

- ✓ **NOTE** Turning the Bluetooth radio on and off using the following procedures is only available on OEM version 05.30.0000 and higher. Earlier OEM versions use StoneStreet API commands to turn the Bluetooth radio on and off. See the *SDMDK Help File* for more information.

Turn off the Bluetooth radio to save power or if entering an area with radio restrictions (e.g., an airplane). When the radio is off, the wearable terminal can not be seen by or connected to other Bluetooth devices. Turn on the Bluetooth radio to exchange information with other Bluetooth devices (within range). Communicate only with Bluetooth radios in close proximity.

- ✓ **NOTE** To achieve the best battery life in wearable terminals with multiple radios, turn off the radios that are not being used.

Disabling Bluetooth

To disable Bluetooth, press **ALT - B**. Use the navigation keys to select **Disable Bluetooth**. Press **ENTER**. An exclamation point appears on the Bluetooth icon indicating that the Bluetooth radio is disabled.

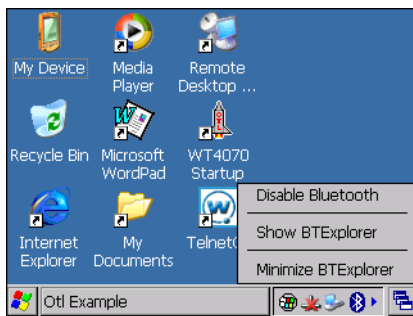


Figure 6-1 *Disable Bluetooth*

Enabling Bluetooth

To enable Bluetooth, press **ALT - B**. Use the navigation keys to select **Enable Bluetooth**. Press **ENTER**. The **Bluetooth** icon changes to indicate that Bluetooth is enabled.

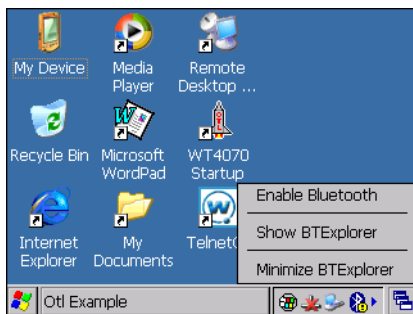


Figure 6-2 *Enable Bluetooth*

Bluetooth Power States

Cold Boot

When a cold boot is performed on the wearable terminal, Bluetooth turns off. It is normal to see the **Bluetooth** icon appear and disappear, as well as a wait cursor, when initialization proceeds in all modes.

Warm Boot

When a warm boot is performed on the wearable terminal, Bluetooth returns to the disabled state (off).

Suspend

When the wearable terminal suspends, Bluetooth turns off.

- ✓ **NOTE** When the wearable terminal is placed in suspend mode, the Bluetooth radio mode powers off and the piconet (Bluetooth connection) is dropped. When the wearable terminal resumes, it could take up to 10 seconds for the Bluetooth radio driver to re-initialize the radio.

Resume

When the wearable terminal resumes, Bluetooth turns on if it was on prior to suspend. Note that any Bluetooth connection that was dropped during a suspend needs to be reconnected after a resume.

Bluetooth Profiles

- ✓ **NOTE** BT Profile Selector application is available on OEM version 05.30.0000 and higher only.

The wearable terminal is loaded with a number of Bluetooth services profiles. These profiles can be loaded or removed from memory. If a profile is not used, it can be removed to save memory. To load or remove profiles:

- ✓ **NOTE** Bluetooth must be disabled prior to changing profiles.

1. If **BTEplorer** is running, press **ALT - B**.
2. Use the navigation keys to select **Disable Bluetooth** and then press **ENTER**.
3. Open **BTProfileSelector** using the **Start** menu:
 - a. Press **CTRL - ESC** to open the **Start** menu.
 - b. Use the navigation keys to highlight **Programs**.
 - c. Press the right arrow key to open the **Programs** menu.
 - d. Use the navigation keys to highlight **BTProfileSelector**.
 - e. Press **Enter**.
4. or using the **Start Up Window App Launcher**:
 - a. Press **5** to access the Utilities screen.
 - b. Press **4** to open the Profile Selector.

5. The **ProfileSelector** window appears.

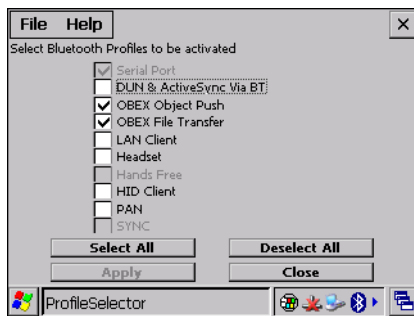


Figure 6-3 Bluetooth Profile Selector Window

✓ **NOTE** The Serial Port profile is always active and cannot be removed.

6. Use the navigation keys to highlight a profile. Press the **SPACE** key to select the profile.
or press **TAB** to place focus on the **Select All** button to select all profiles or the **Deselect All** button to deselect all profiles.
7. Press **TAB** to place focus on the **Apply** button.
8. Press **Space** or **ENTER** to apply any changes.
9. Press **TAB** to place focus on the **Close** button.
10. Press **Space** to exit **Profile Selector**.
11. Press **ALT - B**. Use the navigation keys to select **Enable Bluetooth** to enable the *BTEplorer* application.

See [Services Tab on page 6-23](#) for more information on selecting services.

Accessing BTE Explorer

✓ **NOTE** BTE Explorer is only available on OEM version 05.30.0000 and higher.

The BTE Explorer application can be accessed from the App Launcher menu or by a key combination.

Using App Launcher

In the **App Launcher** main menu, press **5** to select **5 - Utilities**. Press **3** to select **BT Explorer**.



Figure 6-4 App Launcher Screens

Using Key Combination

Press **ALT - B**. Use the navigation keys to select **Show BTE Explorer**.

BTE Explorer Navigation

The WT4090 is a key-based device and navigation within the BTE Explorer application is performed using the keypad.

Table 6-1 Function Keys

Action Key	Key Combination
ALT	Blue key - CTRL
MENU	Blue key - TAB
SPACE	Blue key - BKSP
Left arrow	Blue key - up arrow
Right arrow	Blue key - down arrow

Refer to the *WT4070/90 Wearable Terminal User Guide* for detailed information on keypad navigation.

Key Combinations

The wearable terminal uses special key combinations to easily navigate applications. [Table 6-2](#) lists the key combinations required to perform various application navigation and control functions.

Table 6-2 Key Combinations

Action	Combination
Access the Start menu on the taskbar	CTRL - ESC
Switch fields within an application	TAB
Close windows or cancel operations on some applications	ESC or ALT - F4
Access the Task Manager	ALT - TAB
Switches to the next window or desktop	ALT - ESC
Access a menu bar in an application	ALT - ALT
Press a button or select a check box in an application	TAB until the item is highlighted then SPACE .
Display a pop-up context menu	MENU

Discovering Bluetooth Device(s)

Follow the steps below to discover Bluetooth devices. The wearable terminal can receive information from discovered devices, without bonding. However, once bonded, an exchange of information between the wearable terminal and a bonded device occurs automatically when the Bluetooth radio is turned on.

To find Bluetooth devices in the area:

1. Ensure that Bluetooth is enabled on both devices.
2. Ensure that the Bluetooth device being looked for is in discoverable mode.
3. Ensure that the two devices are within 30 feet (10 meters) of one another.
4. Press **ALT - B**. Use the navigation keys to select **Show BTEplorer**.
5. Press **ENTER**. The **BTEplorer** window appears.

✓ **NOTE** If favorite connections have already been created, the **Favorites** screen displays. If no favorite connections have been created, the **New Connection Wizard** screen displays.

6. From the **Favorite** window:
 - a. Press **ALT - F** to open the **File** menu.
 - b. Use the navigation keys to select **New Connection** and press **ENTER**. The **New Connection Wizard** window appears.



Figure 6-5 *New Connection Wizard Window*

7. Use the navigation keys to select **Explore Services on Remote Device**.

The following actions are available in the drop-down list (actions may vary depending upon configurations):

- Explore Services on Remote Device
- Pair with a Remote Device
- Active Sync via Bluetooth
- Browse Files on Remote Device
- Connect to Headset
- Connect to Internet using Access Point
- Connect to Internet using Phone/Modem
- Connect to Personal Area Network
- Connect to Printer
- Send or Exchange Objects
- Associate Serial Port.

✓ **NOTE** If a device discovery action has not been previously performed, a device discovery is automatically initiated. If a device discovery has previously been performed, the device discovery process is skipped, and the previously found list of devices displays. To start a new device discovery, press **Menu** select **Discover Devices** from the menu and press **ENTER**.

8. Press **ENTER**. **BTE Explorer** searches for Bluetooth devices in the area and displays the devices in the **Select Remote Device** window.



Figure 6-6 *Device Discovery Dialog Box*

- ✓ **NOTE** To filter devices in the list press **ALT - F** to open the filter menu. Select a device type and then press **ENTER**.
To change the display view press **ALT - V** to open the view menu. Select a view type and then press **ENTER**.

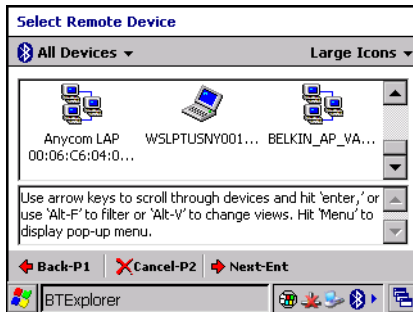


Figure 6-7 Select Remote Device Window

9. Use the navigation keys to select a device from the list and press **ENTER**. The wearable terminal searches for services on the selected Bluetooth device.

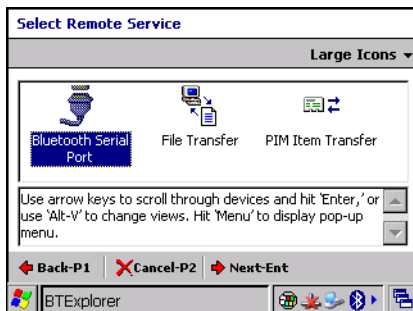


Figure 6-8 Device Services

10. Use the navigation keys to select a service from list and press **ENTER**. The **Connection Favorite Options** window appears.

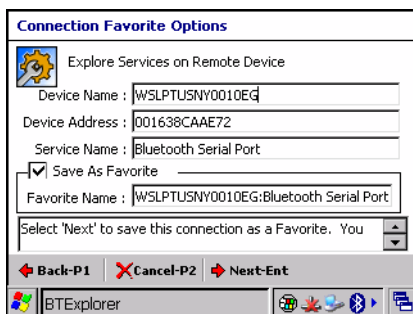


Figure 6-9 Connection Favorite Options Window

11. Press **TAB** to highlight the **Favorite Name** text box, enter a name for this service that will appear in the **Favorite** window.
12. Press **ENTER**. The **Connection Summary** window appears.

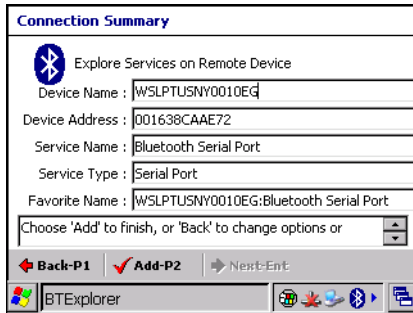


Figure 6-10 Connection Summary Window

13. Press **P2** to add the service to the **Favorite** window.

14. The **Favorite** window appears and the wearable terminal connects to the remote device.

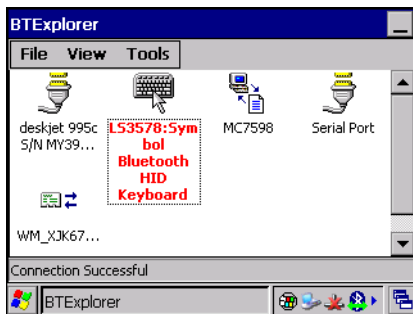


Figure 6-11 Favorite Window with Active Connection

Available Services

Some examples of available services are:

- File Transfer Services
- Headset Services
- OBEX Object Push Services
- Serial Port Services
- Personal Area Network Services
- HID Services.

These services are discussed in the following paragraphs.

File Transfer Services

✓ **NOTE** Shared folders are a security risk.

To transfer files between the wearable terminal and another Bluetooth enabled device:

1. In the **Favorite** window, use the navigation keys to select the file transfer service.
2. Press **MENU** and select **Connect** from the pop-up menu.

3. Press **ENTER**. The **File Transfer** window appears listing the folders of the remote device.

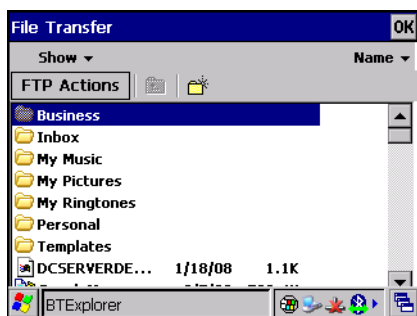


Figure 6-12 File Transfer Window

4. Use the navigation keys to select a file. To open a folder press **ENTER**.
5. Press **ENTER** to copy the file from the remote device. The **Save Remote Device** window appears.

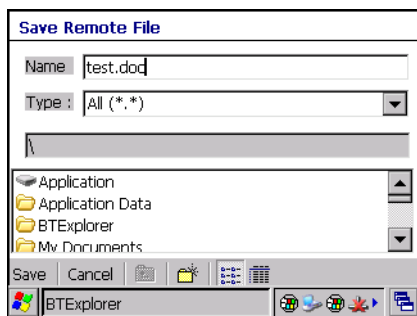


Figure 6-13 Save Remote File Window

6. Press **TAB** three times to enter the folder area.
7. Use the navigation keys to select a folder to place the file into.
8. Press **ENTER**.
9. Press **ENTER** to save the file.
10. Select the action to perform:
 - a. **New** - create a new file or folder on the remote device.
 - b. **Delete** - delete the selected file on the remote device.
 - c. **Get File** - copy the file from the remote device to the wearable terminal.
 - d. **Put File** - copies a file from the wearable terminal to the remote device.
 - e. **Parent Directory** - opens the higher level folder.
 - f. **Refresh** - re-displays the files in the current folder.

Create New File or Folder

To create a new folder or file on the remote device:

1. Press **MENU** to open the pop-up menu.
2. Use the navigation keys to select **New**.

3. Press the right arrow to open the sub-menu.
4. Use the navigation keys to select **Folder** or **File**.
5. Press **ENTER**. The **Create New Folder** or **Create New File** window appears.

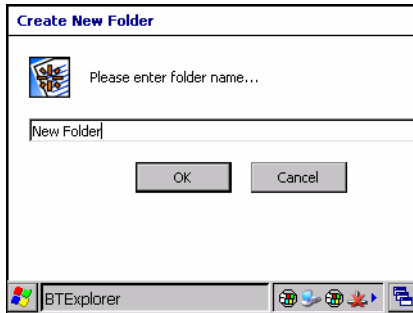


Figure 6-14 Create New Folder Window

6. Enter a new name for the new folder or file and then press **ENTER**.
7. A new folder or file is created on the remote device.

Delete File

To delete a file from the remote device:

1. Use the navigation keys to select the file to delete.
2. Press **MENU** to open the pop-up menu.
3. Use the navigation keys to select **Delete**.
4. Press **ENTER**. A **Delete Remote Device File** dialog box appears.
5. Press **ENTER** to delete the file.

Get File

To copy a file from a remote device to the wearable terminal:

1. Press **MENU** to open the pop-up menu.
2. Use the navigation keys to select **Get**.
3. Press **ENTER**. The **Save Remote File** window appears.

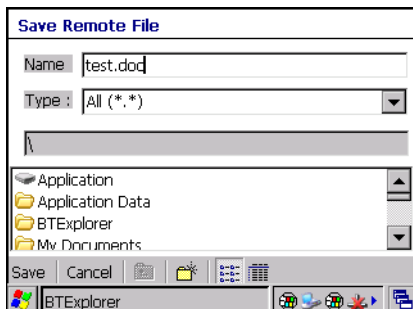


Figure 6-15 Save Remote File Window

4. Press **TAB** three times to enter the folder area.
5. Using the navigation keys to highlight a folder and press **ENTER**. The **OBEX Object Push** window appears.
6. Press **ENTER**. The file is transferred from the remote device to the wearable terminal.

Put File

To copy a file from the wearable terminal to a remote device:

1. In the **File Transfer** window, navigate to a folder where the file will be put into.
2. Press **MENU** to open the pop-up menu.
3. Use the navigation keys to select **Put**.
4. Press **ENTER**. The **Send Local File** window appears.

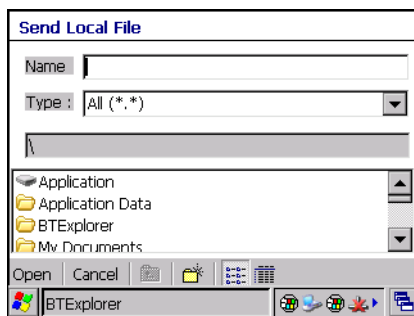


Figure 6-16 Send Local File Window

5. Press **TAB** three times to enter the folder area.
6. Select a file in the wearable terminal.
7. Press **ENTER**. The **Sending Local File** window appears.

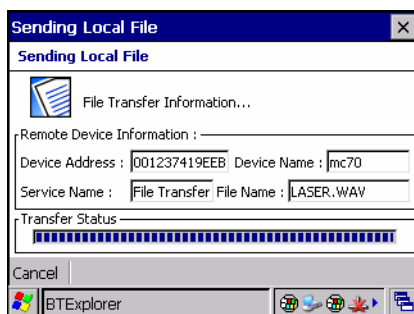


Figure 6-17 Sending Local File Window

8. The file is transferred from the wearable terminal to the remote device.

Connect to Internet Using Access Point

This section explains how to access a Bluetooth-enabled LAN access point (AP) for a network connection. With this method of communication the Internet Explorer can be used to connect to a server.

1. In the **Favorite** window, use the navigation keys to select the LAN Access service.
2. Press **MENU** and select **Connect** from the pop-up menu.

3. Press **ENTER**.
4. The wearable terminal connects with the Access Point.
5. Press **CTRL - ESC** to open the **Start** menu.
6. Use the navigation keys to select **Internet Explorer**.
7. Press **ENTER**. The **Internet Explorer** window appears.
8. In the address field, enter an internet address and tap the **Enter** button. The web page loads.

OBEX Object Push Services

Object Exchange (OBEX) is a set of protocols allowing pictures to be shared using Bluetooth. To send a picture to another device:

1. In the **Favorite** window, use the navigation keys to select the OBEX Push service.
2. Press **MENU** and select **Connect** from the pop-up menu.
3. Press **ENTER**. The **OBEX Object Push** window appears.

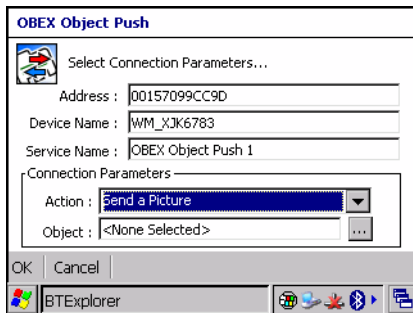



Figure 6-18 OBEX Object Push Window

4. Press **TAB** twice to highlight the  button.
5. Press **SPACE**.
6. The **Send Local Picture** window appears.

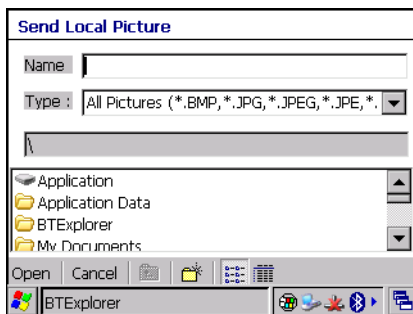


Figure 6-19 Send Local Picture Window

7. Press **TAB** three times to enter the folder area.
8. Using the navigation keys to highlight a file and press **ENTER**. The **OBEX Object Push** window appears.
To open a folder, highlight the folder and press **ENTER**.

9. Press **ENTER**. The wearable terminal connects to the remote device and begins to send the file. The **Sending Picture** window appears. When the file transfer is complete a confirmation dialog appears. Press **ENTER**.

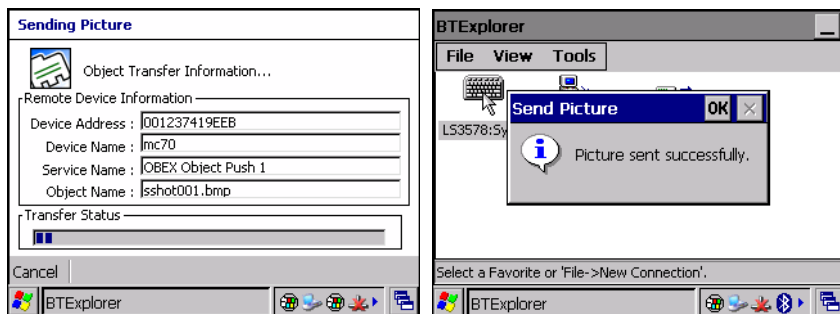


Figure 6-20 Sending Picture Window

Headset Services

To connect to a Bluetooth headset:

1. In the **Favorite** window, use the navigation keys to select the headset service.
2. Press **MENU** and select **Connect** from the pop-up menu.
3. Press **ENTER**.
4. The wearable terminal connects to the headset. Refer to your headset user manual for instruction on communicating with a Bluetooth device.

Serial Port Services

- ✓ **NOTE** By default, COM ports COM4, COM5 and COM9 are Bluetooth virtual ports. If an application opens one of these ports, the Bluetooth driver activates and guides you through a Bluetooth connection.

Use the wireless Bluetooth serial port connection just as you would a physical serial cable connection. You must configure the application that will use the connection to the correct serial port.

To establish a serial port connection:

1. In the **Favorite** window, use the navigation keys to select the Serial Port service.
2. Press **MENU** and select **Connect** from the pop-up menu.
3. Press **ENTER**.
4. The **Remote Service Connection** window appears.

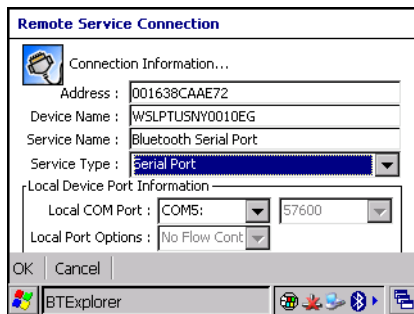


Figure 6-21 Remote Service Connection Window

5. In the **Local COM Port** drop-down list select a COM port.
6. Press **ENTER**.

Personal Area Network Services

Connect two or more Bluetooth devices to share files and collaborate.

To establish a Personal Area Network connection:

1. In the **Favorite** window, use the navigation keys to select the Personal Area Network service.
2. Press **MENU** and select **Connect** from the pop-up menu.
3. The wearable terminal connects to the Personal Area Network.

HID Services

Connect input devices such as Bluetooth keyboards and mice to the wearable terminal.

To establish a HID connection:

1. In the **Favorite** window, use the navigation keys to select the HID service.
2. Press **MENU** and select **Connect** from the pop-up menu.
3. The wearable terminal connects to the HID device.

Bonding with Discovered Device(s)

A bond is a relationship created between the wearable terminal and another Bluetooth device in order to exchange information in a secure manner. Creating a bond involves entering the same PIN on the two devices to bond. Once a bond is created, and the Bluetooth radios are turned on, the devices recognize the bond and are able to exchange information without re-entering a PIN.

To bond with a discovered Bluetooth device:

✓ **NOTE** If favorite connections have already been created, the **Favorites** screen displays. If no favorite connections have been created, the **New Connection Wizard** screen displays.

1. Press **ALT - B**. Use the navigation keys to select **Show BTE Explorer**. The **BTE Explorer** window appears.
2. Press **ALT - F** to open the **File** menu.
3. Use the navigation keys to select **New Connection** and press **ENTER**. The **New Connection Wizard** window appears.



Figure 6-22 New Connection Wizard Window

4. Use the navigation keys to select **Pair with Remote Device**.
5. Press **ENTER**. The **BTE Explorer** searches for Bluetooth devices in the area and displays the devices in the **Select Remote Device** window.

✓ **NOTE** Devices discovered previously are listed to save time. To start a new device discovery, press **Menu** select **Discover Devices** from the menu and press **ENTER**.

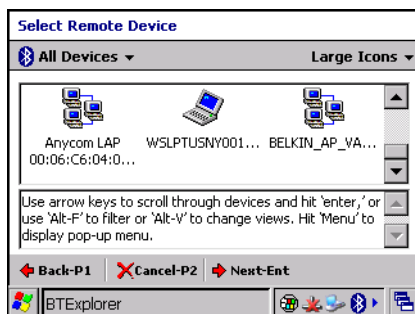


Figure 6-23 Select Remote Device Window

- ✓ **NOTE** To filter devices in the list press **ALT - F** to open the filter menu. Select a device type and then press **ENTER**.
To change the display view press **ALT - V** to open the view menu. Select a view type and then press **ENTER**.

- Use the arrow keys to select a device from the list and press **ENTER**. The **PIN Code Request** window appears.

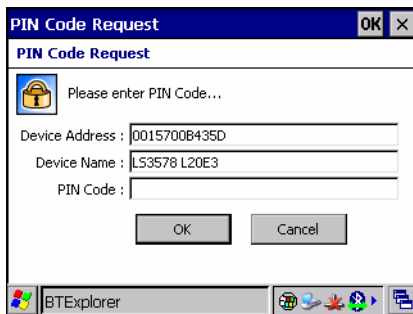


Figure 6-24 Connection Favorite Options Window

- In the **PIN Code** field, enter the PIN code.
- Press **ENTER**. The **Pairing Status** window displays.



Figure 6-25 Pairing Status Window

- Press **P2**. The devices are successfully paired. The device name moves to the **Trusted Devices** window.

Accepting a Bond

When a remote device wants to bond with a wearable terminal, you give permission by entering a PIN when requested.

- Ensure that the wearable terminal is set to discoverable and connectable. See [Bluetooth Settings on page 6-23](#).
- When prompted to bond with the remote device the **PIN Code Request** window appears.

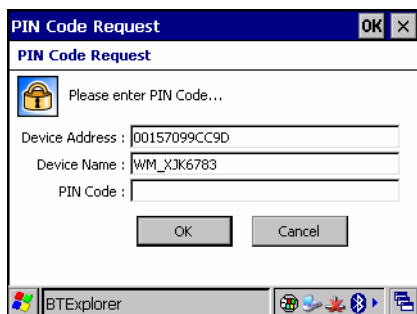


Figure 6-26 PIN Code Request Window

✓ **NOTE** Connections to untrusted devices are a security risk.

3. In the **PIN Code:** text box, enter the same PIN that was entered on the device requesting the bond. The PIN must be between 1 and 16 characters.
4. Press **ENTER**. The bond is created and the wearable terminal can now exchange information with the other device.

Trusted Devices Window

The **Trusted Devices** window lists all bonded devices. To access the **Trusted Devices** window:

1. Launch **BTE Explorer**.
2. Press **ALT - T**.
3. Using the navigation keys select **Trusted Devices**.
4. Press **ENTER**. The Trusted Devices window appears.

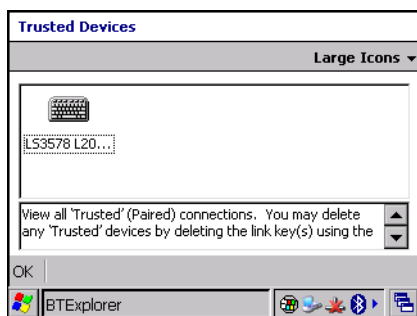


Figure 6-27 Trusted Device Window

The **Trusted Devices** window contains one menu that can be accessed through key combinations. It allows you to change the window listing. To open the **View** menu press **ALT - V**. The menu drop-down list appears.

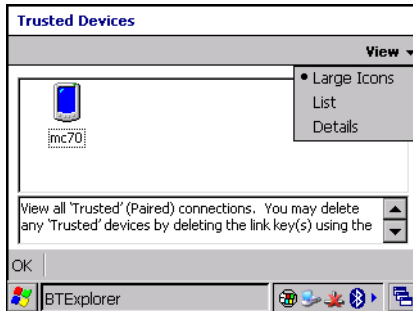


Figure 6-28 *Trusted devices Window Menu*

Use the navigation keys to select a view type and then press **ENTER**.

Deleting a Bonded Device

If it is no longer necessary to connect with a device, delete it from the **Bluetooth Trusted Devices** window.

1. Use the navigation keys to select a device.
2. Press **MENU**.
3. Use the navigation keys to select **Delete Link Key**.
4. Press **ENTER**. A confirmation dialog box appears.
5. Press **ENTER** to confirm deletion of the trusted device.
6. Press **ENTER** to exit the **Trusted Device** window.

Connecting to a Favorite Service

The **Favorite** window can display many services set as favorites. To connect to one of these services:

1. Use the navigation keys to select the service.
2. Press **ENTER**.
3. The wearable computer connects to the service. The service icon text becomes highlighted.

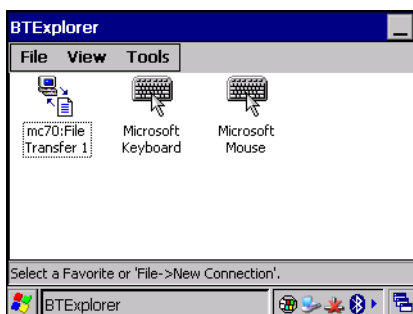


Figure 6-29 *Favorite Window*

To disconnect from a connected service:

1. Use the navigation keys to select the highlighted service.

2. Press **MENU**.
3. Use the navigation keys to select **Disconnect**.
4. Press **ENTER**. A deaconate confirmation dialog box appears.
5. Select **Yes** to disconnect the service. The wearable computer disconnects from the service.

Navigating the Favorites Window

The **Favorites** window has three menus that can be accessed through key combinations.

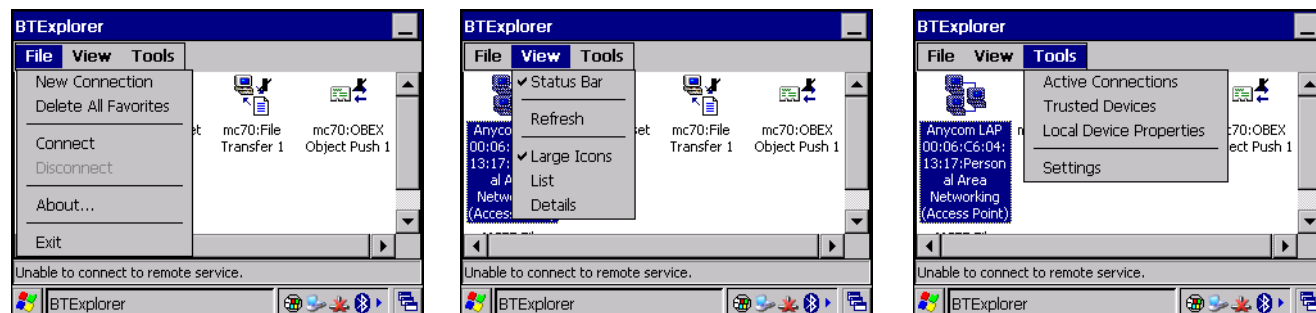


Figure 6-30 Favorites Window Menus

To open the **File** menu, press **ALT - F**.

To open the **View** menu, press **ALT - V**.

To open the **Tools** menu, press **ALT - T**.

Delete all Favorite Services

To delete all favorites from the **Favorites** window:

1. Press **ALT - F**.
2. Use the navigation keys to select **Delete All Favorites**.
3. Press **ENTER**. A confirmation dialog box appears.
4. Press **ENTER** to confirm the deletion or **ESC** to cancel the deletion.

Delete a Favorite Service

To delete a selected favorite:

1. Use the navigation keys to select a favorite.
2. Press **MENU**. The pop-up menu appears.
3. Use the down arrow key to select **Delete**.
4. Press **ENTER**. A confirmation dialog box appears.
5. Press **ENTER** to confirm the deletion or **ESC** to cancel the deletion.

Rename a Favorite Service

To rename a favorite:

1. Use the navigation keys to select a favorite.
2. Press **MENU**.
3. Use the down arrow key to select **Rename**.
4. Press **ENTER**. The **Change Device Name** window appears.
5. Enter a new name.
6. Press **ENTER** to change the name or **ESC** to cancel the name change.

Change the Display View

To change the display view:

1. Press **ALT - V**.
2. Use the down arrow key to select **Large Icons**, **List** or **Details**.
3. Press **ENTER**. The **Favorite** window layout changes.

View Active Connections

To view active connections:

1. Press **ALT - T**.
2. Use the down arrow key to select **Active Connections**.
3. Press **ENTER**. The **Active Connections** window appears.

✓ **NOTE** To filter devices in the list press **ALT - F** to open the filter menu. Select a device type and then press **ENTER**.
To change the display view press **ALT - V** to open the view menu. Select a view type and then press **ENTER**.

4. Press **ENTER** to close the window.

View Properties

To view the properties of the wearable terminal:

1. Press **ALT - T**.
2. Use the down arrow key to select **Local Device Properties**.
3. Press **ENTER**. The **Local Device Property** window appears.
4. Press **ENTER** to close the window.

Bluetooth Settings

Use the **BTE Explorer Settings** window to configure the operation of the **BTE Explorer** application. To access the settings, press **ALT - T**, use the navigation keys to select **Settings**. Press **ENTER**. The **BTE Explorer Settings** window appears.

Use the left and right arrows to move from one tab to the next. Within a tab, use the **TAB** key to move from one field to the next.

Device Info Tab

Use the **Device Info** tab to configure the wearable terminal's Bluetooth connection modes.

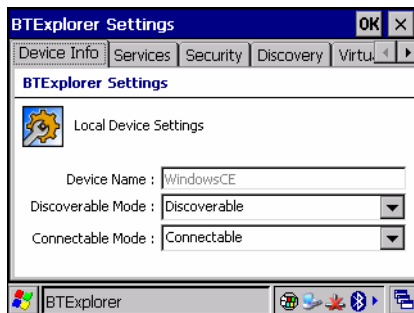


Figure 6-31 BTE Explorer Settings - Device Info Tab

Press **TAB** to move to the next field.

Table 6-3 Device Info Tab

Field	Description
Device Name	Displays the name of the wearable terminal. Not editable.
Discoverable Mode	Allows you to set the wearable terminal to be discoverable by other Bluetooth devices or not be discoverable. Note: For security reasons, the default is set to Non Discoverable .
Connectable Mode	Allows you to set the wearable terminal to be connectable by other Bluetooth devices or not be connectable. Note: For security reasons, the default is set to Non Connectable .

Services Tab

✓ **NOTE** For security reason, by default services are not enabled.

Use the **Services** tab to management of the services the wearable terminal makes available for use by other Bluetooth devices.

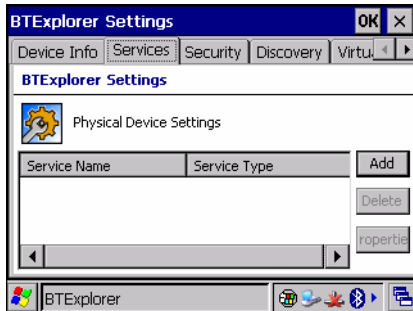


Figure 6-32 BTE Explorer Settings - Services Tab

To add a service:

1. Press **TAB** to highlight the **Add** key. Press **SPACE**. The **Add Local Service** window displays.

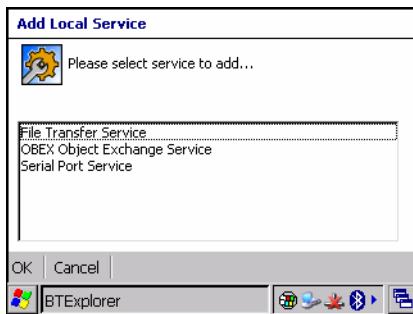


Figure 6-33 Add Local Service Window

2. In the list, use the navigation key to select a service to add.
3. Press **ENTER** to accept the service. Press **ESC** to exit without saving.
The **Edit Local Service** window displays for the selected service.
4. Select the appropriate information and then Press **ENTER**. See the following paragraphs for detailed information on the available services.

File Transfer Service

File transfer allows files to be browsed by other Bluetooth devices.

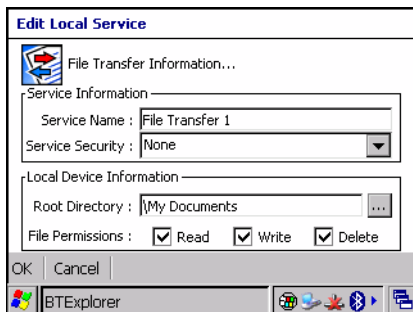


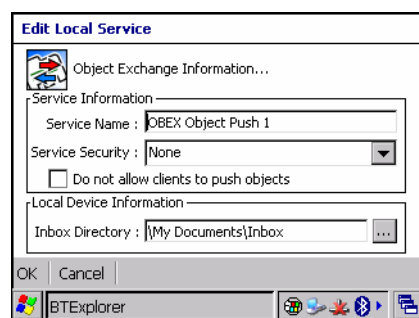
Figure 6-34 File Transfer Information Window

Table 6-4 File Transfer Information Window

Field	Description
Service Name	Displays the name of the service.
Service Security	Select the type of security from the drop-down list; None, Authenticate or Authenticate/Encrypt.
Root Directory	Select the directory that other Bluetooth devices can access.
File Permissions	Select the file permissions for the selected directory. Check the appropriate box to grant Read access, write access and delete access.

OBEX Object Push Service

OBEX Object Push allows contacts, business cards, pictures, appointments, and tasks to be pushed to the device by other Bluetooth devices.

**Figure 6-35** OBEX Exchange Information Window**Table 6-5** OBEX Exchange Information Window

Field	Description
Service Name	Displays the name of the service.
Service Security	Select the type of security from the drop-down list; None , Authenticate or Authenticate/Encrypt .
Business Card	Select a contact information to another mobile device.
Do not allow clients to push objects	Disables clients from pushing objects to the wearable terminal.
Inbox Directory	Select a directory where another Bluetooth device can store files.

Personal Area Networking Service

Personal Area Networking hosts a Personal Area Network which allows communication with other Bluetooth devices.



Figure 6-36 Personal Area Networking Window

Table 6-6 Personal Area Networking Window

Field	Description
Service Name	Displays the name of the service.
Service Security	Select the type of security from the drop-down list; None , Authenticate or Authenticate/Encrypt .
Support Group Ad-Hoc Networking	Select to enable Ad-Hoc networking.

Serial Port Service

Serial port allows COM ports to be accessed by other Bluetooth devices.

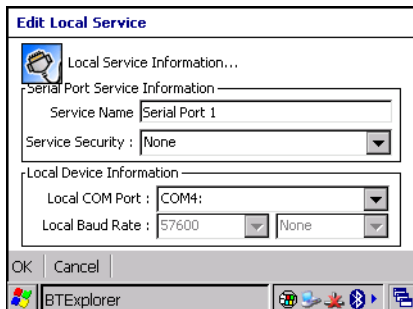


Figure 6-37 Serial Port Service Window

Table 6-7 Serial Port Service Window

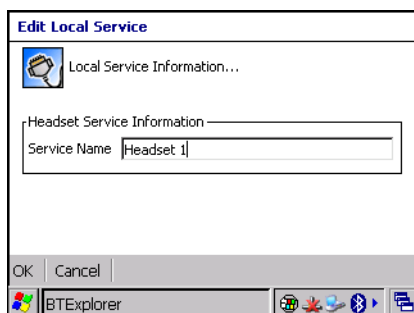
Field	Description
Service Name	Displays the name of the service.
Service Security	Select the type of security from the drop-down list; None , Authenticate or Authenticate/Encrypt .

Table 6-7 Serial Port Service Window

Field	Description
Local COM Port	Select the COM port. Select COM1 to use a modem or other device that is connected to the connector on the bottom of the wearable terminal.
Local Baud Rate	Select the communication baud rate.
Local Port Options	Select the port option.

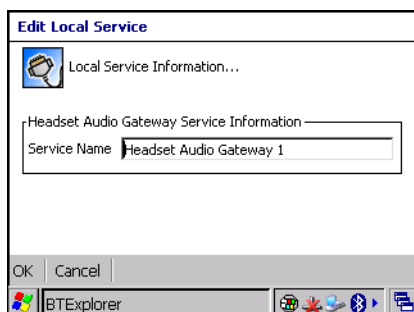
Headset Service

Headset service allows connection to a Bluetooth headset.

**Figure 6-38** Headset Service Window

Field	Description
Service Name	Displays the name of the service.

Headset Audio Gateway Service Information Service

**Figure 6-39** Headset Audio Gateway Service Window

Field	Description
Service Name	Displays the name of the service.

Security Tab

To adjust the security settings for an individual service, select the **Services** tab first, then select the individual service, then **Properties**.

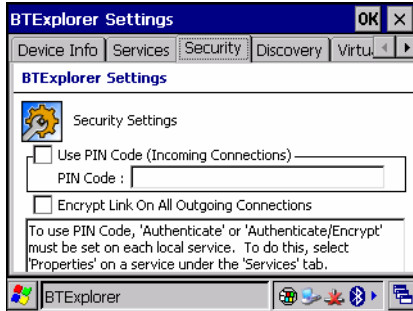


Figure 6-40 BTE Explorer Settings - Security Tab

Table 6-8 Security Tab

Field	Description
Use PIN Code (Incoming Connecting)	Select for automatic use of the PIN code entered in the PIN Code text box. It is recommended not to use this automatic PIN code feature. See Security on page 6-2 for more information.
PIN Code	Enter the PIN code.
Encrypt Link On All Outgoing Connections	Select to enable or disable encryption. Use encryption whenever possible.

Discovery Tab

Use the **Discovery** tab to set and modify discovered devices.

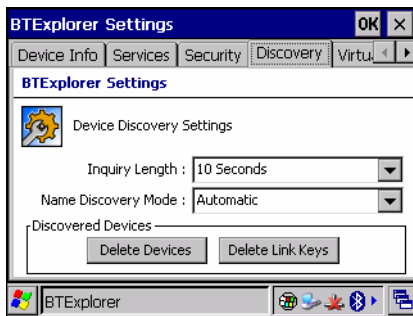


Figure 6-41 BTE Explorer Settings - Discovery Tab

Table 6-9 Discovery Tab

Field	Description
Inquiry Length	Sets the amount of time that the wearable terminal takes to discover Bluetooth devices in the area.
Name Discovery Mode	Select either Automatic or manual .
Discovered Devices buttons	Deletes all discovered devices and link keys.

Virtual COM Port Tab

Use the **Virtual COM Port** tab to select the COM ports for Bluetooth communication.

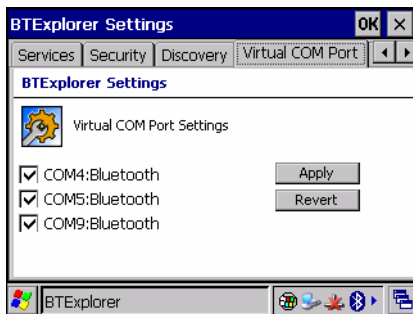


Figure 6-42 BTE Explorer Settings - Virtual COM Port Tab

Table 6-10 Virtual COM Port Screen

Field	Description
COM4:Bluetooth	Enable or disable COM Port 4.
COM5:Bluetooth	Enable or disable COM Port 5
COM9:Bluetooth	Enable or disable COM Port 9



NOTE If an application uses one of the COM ports assigned to Bluetooth, opening this port causes the Bluetooth stack to activate and guide you through the connection process.



Figure 6-43 COM Port Connection

HID Tab

- ✓ **NOTE** The HID tab only appears if HID is selected in the Bluetooth Profile Selector application. See [Bluetooth Profiles on page 6-4](#) for more information.

Use the HID tab to set key repeat settings.

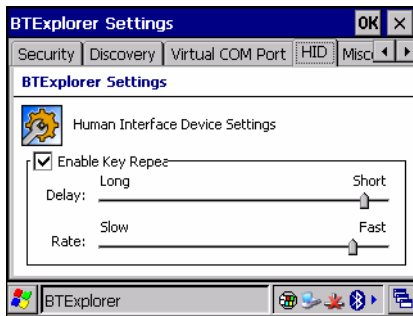


Figure 6-44 BTE Explorer Settings - HID Tab

Table 6-11 HID Tab

Field	Description
Enable Key Repeat	Enable the Delay and Rate settings.
Delay	Sets the amount of time that elapses before a character repeats when you hold down a key.
Rate	Sets the speed at which a character repeats when you hold down a key.

Miscellaneous Tab

Use the Miscellaneous tab to set

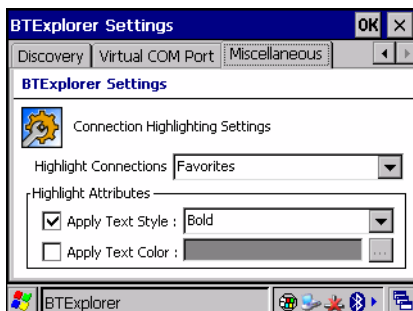


Figure 6-45 BTE Explorer Settings - Miscellaneous Tab

Table 6-12 *Miscellaneous Tab*

Field	Description
Highlight Connections	Select the connection type to highlight when connected. In the Wizard Mode, the only option is Favorites or None .
Apply Text Style	Select the text style to be applied to the connection text.
Apply Text Color	Select the text color to be applied to the connection text.

Chapter 7 Application Deployment

Software Installation on Development PC

To develop applications to run on the wearable terminal, use one or all of the following:

- Enterprise Mobility Developer Kit (EMDK) for C
- Windows CE Platform SDK for WT40x0
- Device Configuration Package (DCP) for WT40x0.

The EMDK for C is a development tool used to create native C and C++ applications for the WT4070/90. It includes documentation, header files (.H), and library files (.LIB) for native code application development that targets Zebra value-add APIs.

✓ **NOTE** Refer to the EMDK WT4090-VOW Programming page for full information on programming the Voice Only WT4090.

The Windows CE Platform SDK for the WT40x0 is used in conjunction with the SMDK for C to create Windows CE applications for the WT40x0 wearable terminal. The Platform SDK installs a new Windows CE device type and its associated libraries onto the development PC.

The Device Configuration Package (DCP) is required to create and download hex images that represent flash partitions to the wearable terminal. The DCP includes the user documentation, flash partitions, Terminal Configuration Manager (TCM) and the associated TCM scripts.

Device Configuration Package

To install the DCP for WT40x0:

1. Download the DCP from the Support Central web site, <http://www.zebra.com/support>:
 - a. On <http://www.zebra.com/support>, select *Software Downloads*.
 - b. Select *Mobile Computers* and then select *WT4000*.
 - c. Select the *Device Configuration Package (DCP)*.
 - d. Save the .exe file to the development computer.
2. Locate the .exe file on the development computer, double-click the file, and follow the install screen prompts.

3. Once installed, access the major components of the DCP from the *Device Configuration Package (DCP)* for *WT40x0* program group of the *Windows Start Menu*.

Platform SDK

Different Platform SDKs are required for the Microsoft® Windows CE 5.0 Professional and Microsoft® Windows CE 5.0 Core platforms. To download and install the appropriate Platform SDK:

1. Download the appropriate Platform SDK from the Support Central web site, <http://www.zebra.com/support>:
 - a. On <http://www.zebra.com/support>, select *Software Downloads*.
 - b. Select *Mobile Computers* and then select *WT4000*.
 - c. Select the *Platform SDK*.
 - d. Save the .exe file to the development computer.
2. Run the file and follow the screen prompts to install.

Enterprise Mobility Developer Kits

To install an EMDK:

1. Download the EMDK from the Support Central web site, <http://www.zebra.com/support>:
 - a. On <http://www.zebra.com/support>, select *Developer Downloads* and sign in.
 - b. Select *Mobile Computers* and then select *WT4000*.
 - c. Select the latest version of the *Symbol Mobility Developer Kit*.
 - d. Download the .exe file to the development computer.
2. Double-click the executable file and follow the install screen prompts.

Installing Other Development Software

Developing applications for the wearable terminal may require installing other development software such as application development environments on the development PC. Follow the installation instructions provided with this software.

Deployment

With the appropriate accessory, software, and connection, the wearable terminal can share information with the host device. This chapter provides information about installing software and files on the wearable terminal.

Download/Install software using:

- OSUpdate
- ActiveSync
- IPL.

OSUpdate

The wearable terminal contains tools that update all operating system components. All updates are distributed as packages and/or hex images. Update packages can contain either partial or complete updates for the operating system. Zebra distributes the update packages on the Support Central Web Site, <http://www.zebra.com/support>.

Update an operating system component using one of the following:

- MSP. See [Chapter 8, Staging and Provisioning](#) for information.
- OSUpdate.

Update Loader

To initiate an update using the wearable terminal temp directory:

1. Go to the Support Central web site, <http://www.zebra.com/support>.
 2. Download the appropriate update package to a host computer.
 3. Connect the wearable terminal to a host computer using the Single Slot Serial/USB Cradle. See [Chapter 2, Accessories](#).
 4. Using ActiveSync, copy the update package to the \temp directory.
- ✓ **NOTE** To control the Voice Only WT4090, it must be connected to a host computer running remote desktop software. See [Chapter 4, Voice Only WT4090 Remote Control](#) for more information.
5. On the wearable terminal, use Windows Explorer to navigate to the temp directory.
 6. Open the OSUpdate folder.
 7. Launch the file: 4000c50Ben_TEMP.Ink file.
 8. When the Update Loader application finds the appropriate file, it loads the package onto the wearable terminal.

- ✓ **NOTE** On the WT4070/90, a progress bar displays until the update completes.

On the Voice Only WT4090, as soon as OSUpdate starts, all three LEDs turn on and then the three LEDs indicate the progress of the download. When 33% is completed the first LED turns on, followed by second LED when 66% is completed and finally the third LED when 100% of the image is downloaded. This process is repeated for each image included in the OSUpdate package. Depending on the size of each image the time taken to indicate this progress may vary.

9. When complete, the wearable terminal re-boots.

ActiveSync

Use ActiveSync to copy files from a host computer to the wearable terminal.

Ensure that ActiveSync is installed and that a partnership has been created, see [Chapter 3, ActiveSync](#).

1. Connect the wearable terminal to the host computer using a USB cradle or an appropriate cable, see [Chapter 2, Accessories](#) for connection information.
2. On the host computer, select **Start > Programs > ActiveSync**.
3. Select **Explore**.

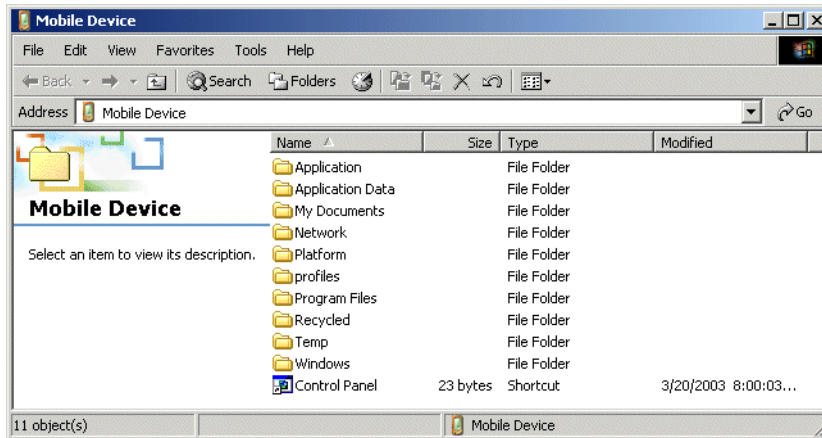


Figure 7-1 ActiveSync Explorer

- Double-click the folder to expand the contents of the folder.

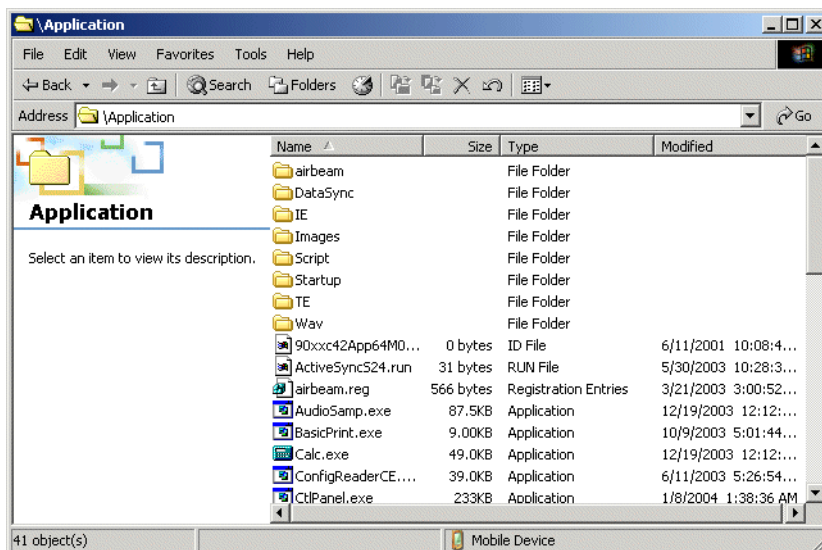


Figure 7-2 My Pocket PC Contents

- Use Explorer to locate the host computer directory that contains the file to download. Tap that directory in the left pane to display its contents in the right pane.
- Drag the desired file(s) from the host computer to the desired mobile device folder.
 - Program Files* folder: files stored in this folder are discarded after a cold boot.
 - Application* folder: files stored in this folder are retained after a cold boot.

IPL

Use IPL to download files onto the wearable terminal, to download customized flash file system partitions to the wearable terminal and load hex files to the flash memory of the wearable terminal.

There are two types of update supported by the wearable terminal: partitions and files. The file system used by the wearable terminal is the same as the file system used on a desktop computer. A file is a unit of data that can be accessed using a file name and a location in the file system. When a file is replaced, only the contents of the

previous file are erased. The operating system must be running for a file to be updated, so the IPL cannot perform individual file updates as it is a stand-alone program that does not require the operating system to be running.

A typical partition is a group of files, combined into a single “partition” that represents a specific area of storage. Examples of partitions are the flash file systems such as *Platform* or *Application*. (Using the desktop computer comparison, these partitions are roughly equivalent to a C: or D: hard disk drive.) In addition to the “hard disk” partitions, some partitions are used for single items such as the operating system, monitor, or splash screen. (Again using a desktop computer comparison, these partitions are roughly the equivalent of the BIOS or special hidden system files.) When a partition is updated, all data that was previously in its storage region is erased - i.e. it is not a merge but rather a replacement operation. Typically, the operating system is not running when partitions are updated, so IPL can perform partition updates.

Partition images for selected partitions can be created by TCM. All partition images suitable for use by IPL are in hex file format for transfer by TCM from the development computer to the wearable terminal.

Upgrade requirements:

- The hex files to be downloaded (on development computer)
- A connection from the host computer and the wearable terminal (either serial or wireless)
- TCM (on development computer) to download the files.

Once these requirements are satisfied, the wearable terminal can be upgraded by invoking IPL and navigating the menus. See [Sending the Hex Image Using IPL on page 7-11](#) for procedures on downloading a hex file to the wearable terminal.

Creating Hex Images

Terminal Configuration Manager (TCM) is an application used to customize flash file system partitions for the wearable terminal. The most common use is to create an application partition hex file that contains the customer's application. TCM can also be used to load hex files to the flash memory of the wearable terminal.

The program resident on the wearable terminal that receives the hex file and burns it to the flash memory is called Initial Program Loader (IPL).

The customization of partitions is controlled by TCM scripts. The scripts contain all of the necessary information for building an image. The script is a list of copy commands specifying the files to copy from the development computer to the partition.

TCM works with a pair of directory windows, one displaying the script and the other displaying the source files resident on the development computer. Using standard windows drag and drop operations, files can be added and deleted from the script window.

The DCP for WT40x0c50 includes scripts used by Zebra to build the standard factory installed *Platform* and *Application* partitions provided on the wearable terminal. The standard *Platform* partition contains drivers while the *Application* partition contains demo applications and optional components. The standard TCM scripts can be found in the following folder: *C:\Program Files\Symbol Device Configuration Packages\WT40x0c50 v1.0\TCM Scripts*.

- ✓ **NOTE** Before creating a script to build a hex image, identify the files required (system files, drivers, applications, etc.) and locate the files' source directories to make the script building process easier.

The required processes for building a hex image in TCM include:

- Starting TCM
- Defining script properties

- Creating the script for the hex image
- Building the image
- Sending the hex image
- Creating a splash screen
- Flash storage.

Starting Terminal Configuration Manager

Click the Windows start menu TCM icon (*Device Configuration Packages, WT40x0c50*) to start TCM. The **TCM** window appears displaying two child windows: **Script1** and **File Explorer**. The **Script1** window contains a newly created script and the **File Explorer** window contains a file explorer view used for selecting files to be placed in the script.

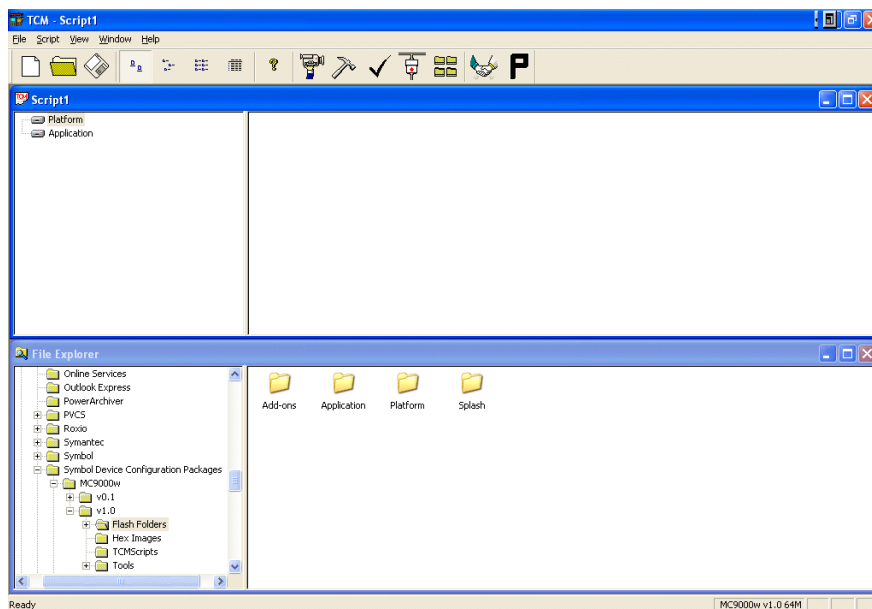


Figure 7-3 TCM Startup Window

The following table lists the components of the TCM window.

Table 7-1 TCM Components


















Icon	Component	Function
	Script Window	Displays the files to be used in the creation of the partition(s).
	File Explorer Window	Used to select the files to be added to the script.
	Create button	Create a new script file.
	Open button	Open an existing script file.

Table 7-1 TCM Components (Continued)

Icon	Component	Function
	Save button	Save the current script file.
	Large icons button	View the current script items as large icon.
	Small icons button	View the current script items as small icon.
	List button	View the current script items as a list.
	Details button	View the current script items with more details.
	About button	Display version information for TCM.
	Properties button	View/change the current script properties.
	Build button	Build the current script into a set of hex files.
	Check button	Check the script for errors (files not found).
	Send button	Download the hex image to the vehicle computer.
	Tile button	Arrange the sub-windows in a tiled orientation.
	Build and Send	Build the current script into a set of hex images and send the hex images to the vehicle computer.
	Preferences button	View/change the global TCM options.

Defining Script Properties

Before a script is created, the script properties must be defined. This defines the type of wearable terminal, flash type, number of disks being created and the memory configuration of each disk partition.

To define the script properties:

1. Select the **Script** window to make it active.
2. Click the **Properties** button. The **Script Properties** window > **Partition Data** tab appears.

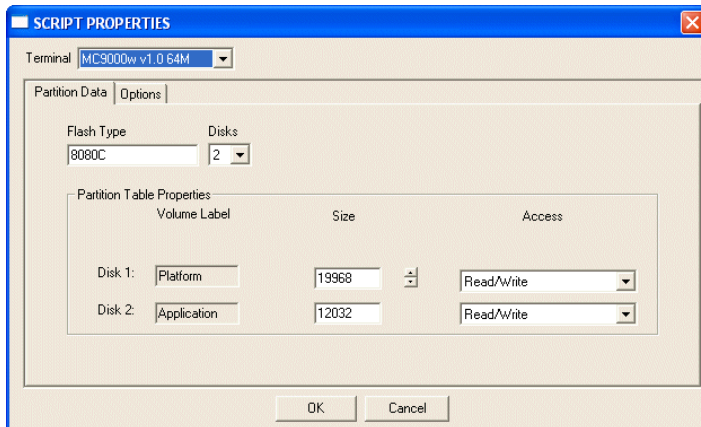


Figure 7-4 Script Properties Window - Partition Data Tab

3. In the **Terminal** drop-down list, select the terminal type.
4. Use the default **Flash Type**.
5. In the **Disks** drop-down list, select the number of disk partitions to create.
6. Select the (memory) **Size** for each partition. Note that adding space to one disk partition subtracts it from another.
7. In the **Access** drop-down list for each disk partition, determine and select the Read/Write access option.
8. Click the **Options** tab. The **Script Properties window Options** tab appears.

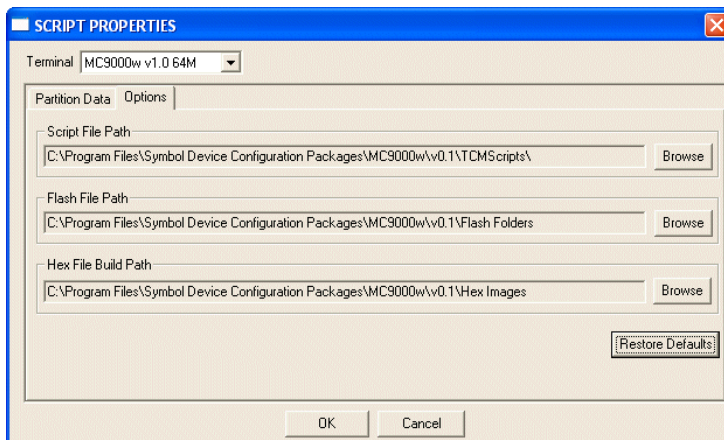


Figure 7-5 Script Properties Window - Options Tab

9. Set the paths for the Script File, Flash File and Hex File Build.
10. Click **OK**.

Creating the Script for the Hex Image

On start-up, TCM displays the TCM window with the **Script1** window and **File Explorer** window pointing to the following directory:

\\Program Files\Symbol Device Configuration Packages\MC40x0c\v0.1\TCMScripts\

The *Script1* window directory pane displays two partitions: *Platform* and *Application*. Depending on the type of flash chip, the number of partitions may change. Files can be added to each of the partitions. TCM functionality includes:

- Opening a new or existing script file
- Copying components to the script window
- Saving the script file.

Opening a New or Existing Script

A script file can be created from scratch or based on an existing script file. Click **Create** to create a new script or click **Open** to open an existing script (for example, a script provided in the DCP for MC40x0c). If an existing script is opened and changes are made, saving the changes overwrites the original script. To use an original or Zebra supplied standard script as a base and save the changes in a new script, use the *Save As* function to save the script using a different file name.

Updating TCM 1.X Scripts

Script files that were created with older versions of TCM can be upgraded to TCM 2.0 scripts. Click **Open** to open an existing script created with an older version of TCM. The *Conversion* window appears automatically.

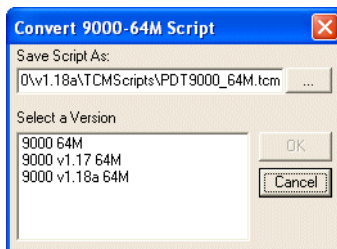


Figure 7-6 Conversion Window - Upgrading to TCM 2.0

Copying Components to the Script

Script contents are managed using standard file operations such as **New Folder**, **Delete** and **Rename**. Items can be added to the script by clicking files and folders in the **File Explorer** window and dragging them to the **Script** window. The **File Explorer** window supports standard windows; multiple files may be selected by clicking while holding the **SHIFT** or **CTRL** keys.

Saving the Script

Modifications to a script file can be saved using the **Save** or the **Save As** function. Saving changes to an existing script writes over the original script. To use a Zebra-supplied standard script as a base and save the changes in a new script, use the **Save As** function.

Building the Image

Once the script is created, the hex image defined by the script can be built.

As part of the build, TCM performs a check on the script which verifies that all files referenced in the script exist. This check is important for previously created scripts to ensure that files referenced in the script are still in the designated locations.

To build scripts:

1. Click **Build** on the TCM toolbar. The **Configure Build** window appears.

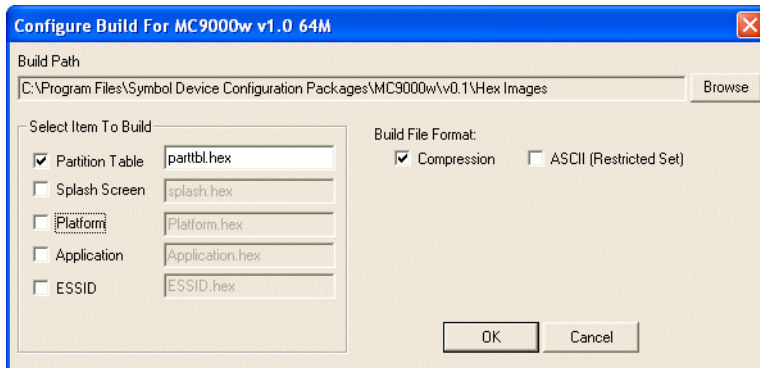


Figure 7-7 *Configure Build Window*

2. Select the items (partitions) to build using the check box(es) to the left of each named partition.
3. The **Build Path** defines where to store all built partitions.
4. Select (hex image) **COMPRESSION** to reduce the size and speed up the download.
5. Click **OK** and follow the on-screen instructions.

If one of the partitions being built is the ESSID, a prompt appears requesting the ESSID value. Deselect the HR (High Rate) check box when building ESSID images for a device with an FH radio.

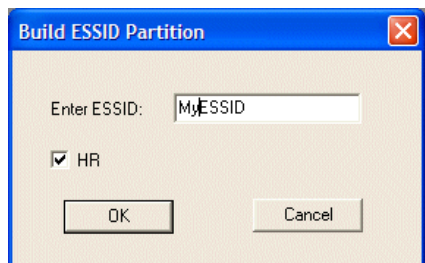


Figure 7-8 *Build ESSID Partition Window*

If one of the partitions being built is the Splash Screen, a prompt appears requesting both the source Bitmap file and the destination HEX file.

6. A check is performed and if there are no errors, the partition hex files are created.

If the build fails, the hex files are not be created and TCM displays an error message. Two of the most common reasons for a build failure are:

- Files defined in the script can not be found. This error can occur when the files referenced by the script are no longer stored on the development computer or the folders where they are stored were renamed.
- The total amount of flash memory space required by the script exceeds the image size. To correct this, reduce the number of files in the partition or increase the size of the partition. See [Defining Script Properties on page 7-7](#) for more information about setting the image size appropriately.

Sending the Hex Image Using IPL

Once the hex file is built, it can be downloaded to the wearable terminal using IPL.

- ✓ **NOTE** The wearable terminal must be inserted in the cradle with appropriate power supply connected to a power source, for the wearable terminal to reset into IPL.

WT4070/90

1. Press the **1, 9** and **Power** button. The wearable terminal performs a cold boot.
2. The screen blanks and three brackets display “} } }”. Immediately press the **P2** key. The **Initial Program Loader** menu displays.

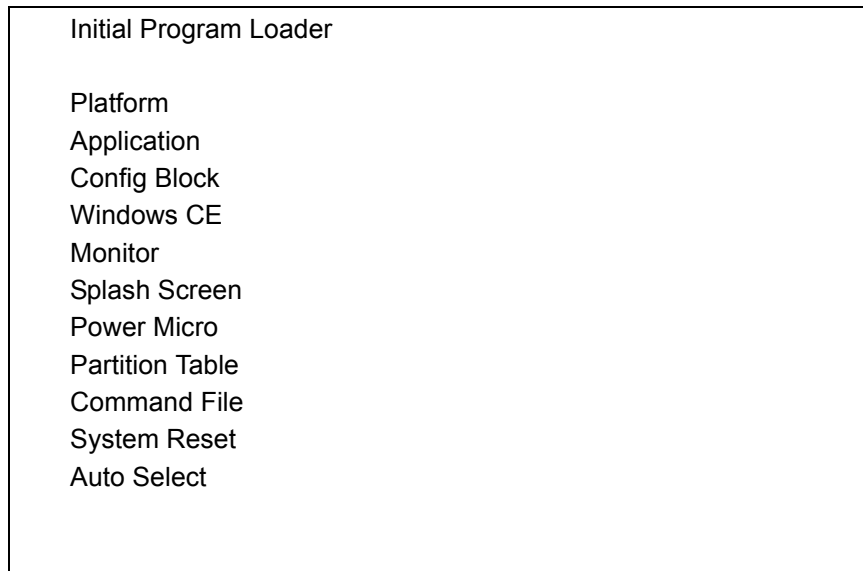


Figure 7-9 Initial Program Loader (IPL) Menu



CAUTION To insure a successful download, do not remove power from the wearable terminal while in IPL mode.

- ✓ **NOTE** The hex images must be downloaded in the following order:
1. Monitor (wearable terminal resets after downloading monitor)
 2. Config Block
 3. Partition Table and Power Micro
 4. Platform, Splash Screen, Application and Windows CE.

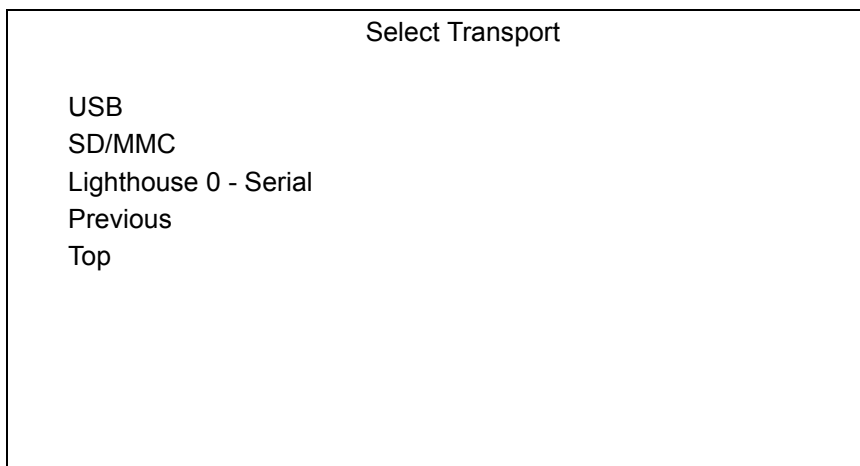
If the platform or application partition sizes are changed, you must download a new partition table first.

3. Choose Auto Select or use the up and down scroll buttons to select the partition to download, then press **Enter**.

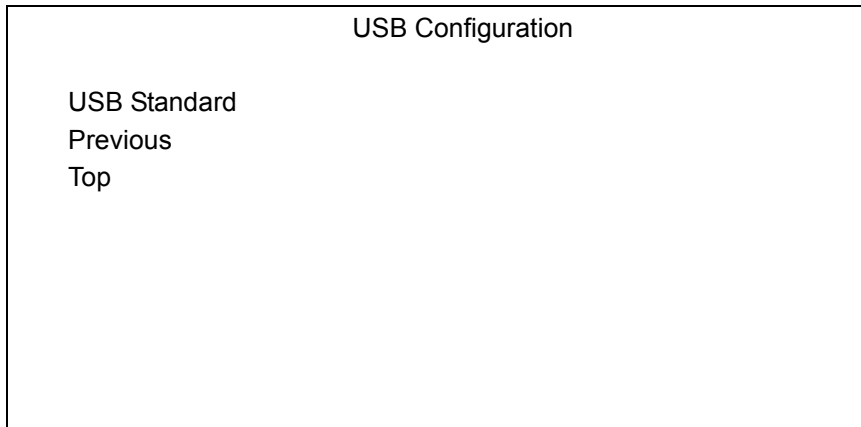
Table 7-2 IPL Menu Partitions

Partition Name	Description
Platform	Contains the files in the <i>Platform</i> folder.
Application	Contains the files in the <i>Application</i> folder.
Windows CE	Contains the operating system for the wearable terminal.
Monitor	Contains the Monitor and IPL programs.
Splash Screen	Contains the splash screen that displays while booting the wearable terminal. Note: Splash screens are generated from .bmp images and must be less than or equal to 240 pixels wide and 296 pixels deep. For color screens the color depth must be 8 bpp. Note: 8 bits per pixel only applies to splash screen images. Once Windows CE is running, the color density is 16 bits per pixel.
Power Micro	The Power Micro is a small computer contained within the wearable terminal that controls several system resources. In the unlikely event that the Power Micro Firmware needs updating, selecting this item allows the device to be programmed.
Partition Table	Contains the partition information for all other partitions. Note: The partition table should never need changing unless the sizes of the platform and application images are changed within TCM. If this is done, then the new partition table should be loaded first, followed by both platform and application in any order.
Command File	Select to load a command file. A command file is a file that allows you to automatically load a number of partitions in a batch process.
System Reset	Selecting this item provides a simple method to exit IPL and to boot the operating system.
Auto Select	Selecting this item allows one or more files to be downloaded without having to manually select the destination. (The content of the files being downloaded automatically directs the file to the correct destination.) For technical reasons, Auto Select cannot be used to download Monitor, Power Micro, or Partition Table. These items must be specifically selected.

4. IPL displays the **Select Transport** menu which lists the available methods of downloading the file.

**Figure 7-10** Select Transport Menu

5. Use the up and down scroll buttons to select **USB** and press **Enter**. If this is the first time using USB transport, you might need to install the Zebra USB driver. Follow the screen prompts.
6. The **USB Configuration** menu appears.



7. Select **USB Standard** and press **ENTER**. The **Download File?** menu appears.

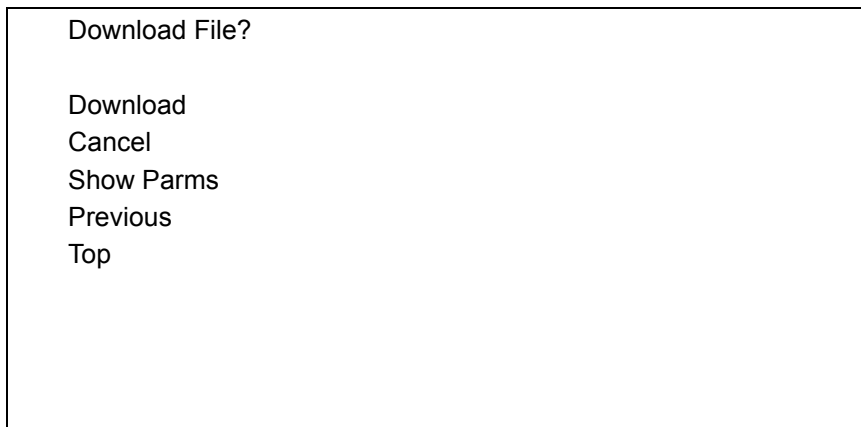


Figure 7-11 *Download File? Menu*

8. Use the up and down scroll buttons to select **Show Parm** to verify the file to download. Press **ENTER** to display the **Parameters** screen.

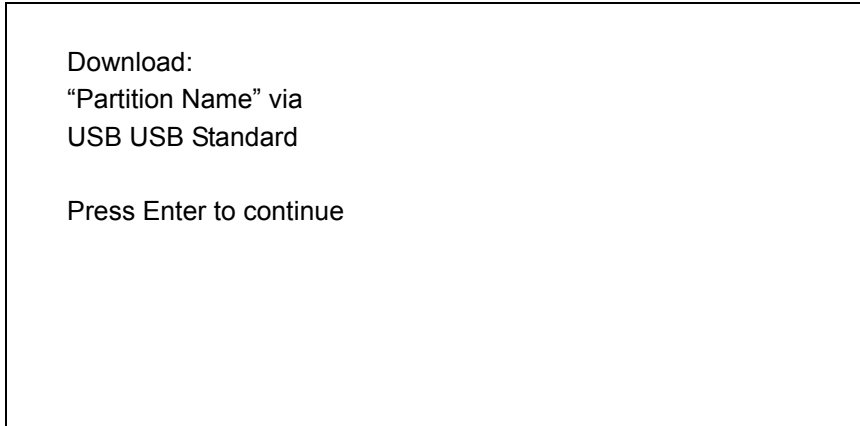


Figure 7-12 Parameters Screen

Partition Name is the name of the partition selected in the **Initial Program Loader** menu.

9. Press **Enter** to return to the **Download File?** menu.
10. Use the up and down scroll buttons to select **Download**. Press **Enter**. The **Downloading** screen appears.

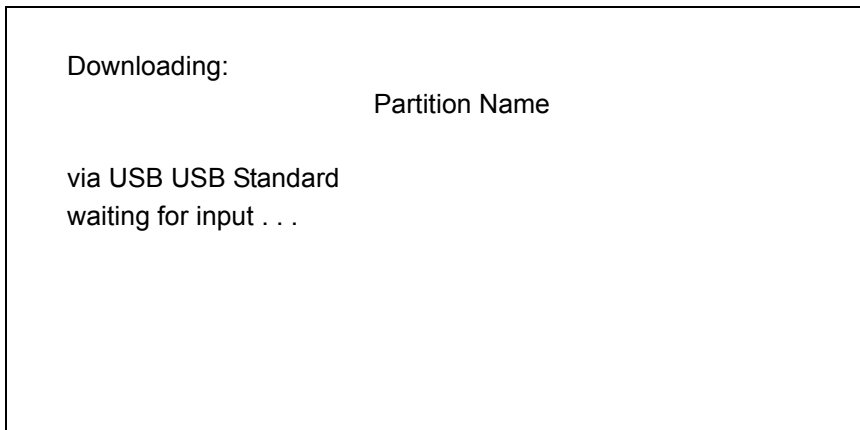


Figure 7-13 Downloading Screen

11. On the development computer, click **Load** on the TCM toolbar. The **Load Terminal** window > **Serial** tab appears.

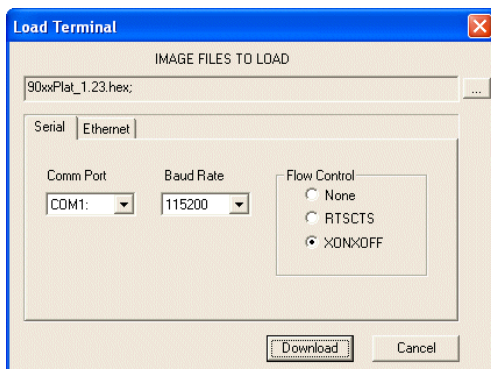


Figure 7-14 Load Terminal Window - Serial and Ethernet Tabs

12. Select the **Image Files To Load**.
13. In the **Comm Port** drop-down list, select **USB: Symbol Device**.
14. Click **Download** to begin the operation.
15. During download, the **Downloading** screen on wearable terminal displays the **Device Status** and a progress bar.
16. When complete, **Device Status** displays **Result was: Success!**, or in the case of an error, the cause of the error.
17. On completion, press **ENTER** to return to the IPL menu to select the next partition to download.
18. To exit IPL, select the **System Reset** item from the IPL menu (see [Figure 7-9 on page 7-11](#)).

Voice Only WT4090

1. Press the **P1** and **P2** keys and **Power** button.
2. The Voice Only WT4090 performs a cold boot.
3. Press the **P2** key. The three LEDs turn on indicating that the Voice Only WT4090 is in IPL mode.
4. On the development computer, click **Load** on the TCM toolbar. The **Load Terminal** window > **Serial** tab appears.

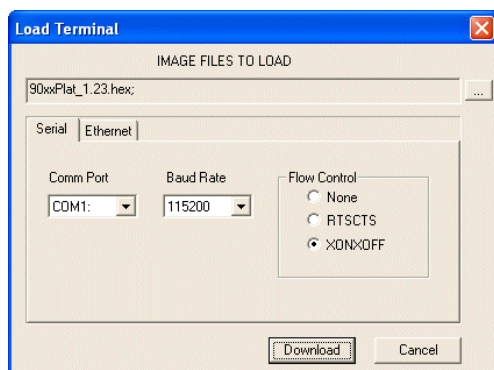


Figure 7-15 Load Terminal Window - Serial and Ethernet Tabs



CAUTION To insure a successful download, do not remove power from the Voice Only WT4090 while in IPL mode.



NOTE The hex images must be downloaded in the following order:

1. Monitor (Voice Only WT4090 resets after downloading monitor)
2. Config Block
3. Partition Table and Power Micro
4. Platform, Splash Screen, Application and Windows CE.

If the platform or application partition sizes are changed, you must download a new partition table first.

5. Select the **Image Files To Load**.
6. In the **Comm Port** drop-down list, select **USB: Symbol Device**.
7. Click **Download** to begin the operation. As soon as the download starts, all three LEDs turn on and then the three LEDs indicate the progress of the download. When 33% is completed the first LED turns on, followed by second LED when 66% is completed and finally the third LED when 100% of the download. Depending on the size of each image the time taken to indicate this progress may vary.

8. When complete, the message “Transfer Complete. Check the terminal for successful completion.”
9. Click **OK**.
10. Repeat steps 5 through 9 for each file to download.
11. To exit IPL, perform a cold boot.

TCM Error Messages

TCM validates the cells in the partition table when the Execute button is clicked. Cells highlighted in red contain an error. Partition loading is disabled until all errors are corrected.

Table 7-3 TCM Error Messages

Error	Description/Solution
Failed to build images: flash file system DLL not loaded!	TCM could not load the DLL required to build images for the targeting flash file system. Reinstall TCM or recover the DLL.
Failure finding directory xxx	Building process failed because directory xxx was not found.
Failure creating volume	Building process failed because a certain disk volume could not be created.
Failure adding system file to image	Build process failed because TCM failed to add a certain system file to the disk image.
INVALID PATH	The path for the image file to build is not valid.
Nothing Selected To Build	In the Config Build window, no item is selected to build.
Illegal ESS ID	In the Build ESSID Partition window, no ESS ID was entered or the ESS ID entered was illegal.
Disk Full	TCM failed to create Hex image file at the selected path. Check available disk space.
Target Disk Full	Build process failed because TCM failed to add file to the image of a disk volume. Remove some files or increase the disk size.
Hex file is READ ONLY	The Hex image file to be created exists and is read-only. Delete the existing file or change its attribute.
Error opening the file xxx with write access	TCM could not open file xxx with write access. Check if file is in use.
Failure creating binary file	TCM failed to open/create an intermediate binary file.
Hex File To load is missing or invalid	In Load Terminal window, the file selected to load has invalid status.
Could not locate wearable terminal name in TCM.ini file	While loading the Script Properties window, TCM could not find the TCM.ini section corresponding to the wearable terminal type specified by the current opening script. Either TCM.ini or the script file is invalid.
Incorrect disk sizes in TCM.ini file	The total disk size specified in the script does not match the total disk size defined in the corresponding TCM.ini section. Check if the script is corrupt or the TCM.ini has changed after the script was created.

Table 7-3 TCM Error Messages (Continued)

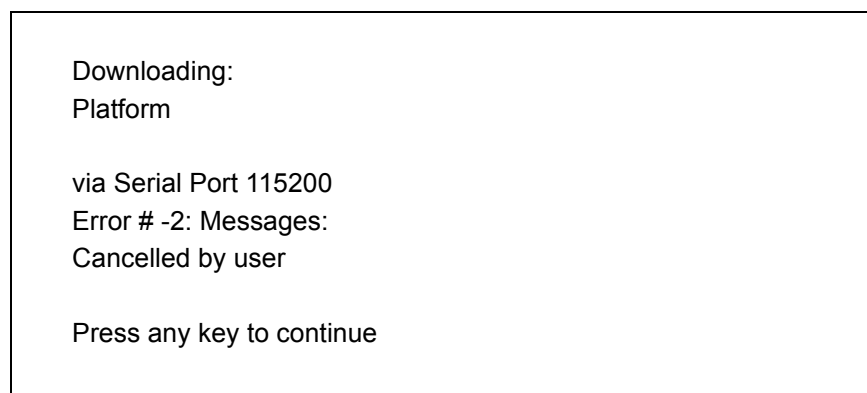
Error	Description/Solution
INVALID DIRECTORY	In Script Properties window, the selected System File Path is not a valid directory.
One of the disk sizes is one sector in size	In Script Properties window, one of the disks is too small (one sector in size). This may cause problem while building images, especially when cushion is enabled. Increase the disk size.
INVALID VOLUME NAME	In Script Properties window, one of the volume labels is not valid.
Corrupt TCM.INI file! (Invalid value of VolumeDivisor)	The VolumeDivisor entry is missing or invalid in the TCM.ini. Reinstall TCM or recover TCM.ini.
Invalid version of TCM script file	The TCM script was not created by this version of TCM.
Corrupt or missing TCM.ini file	TCM could not find TCM.ini file.
FAILED CONNECTION TO COM PORT (Could not get status)	While downloading images to wearable terminal, TCM failed to connect to the selected COM port. Check if the COM port is free and is properly configured.
FAILED CONNECTION TO TERMINAL (Terminal Not Connected Properly/Terminal Not Ready to Receive)	While downloading images, TCM failed to connect to the wearable terminal. Check if the correct flow control protocol is selected and the wearable terminal is properly connected and is in a listening state.

IPL Error Detection

While receiving data, IPL performs many checks on the data to ensure that the data is received correctly. If an error is detected, IPL immediately aborts the download, and reports the error on an error screen on a WT4070/90 or with the LEDs on a Voice Only WT4090.

WT4070/90 Error Indications

Error screens may vary depending on the action being performed. A sample error screen may look like the screen pictured below:

**Figure 7-16** IPL Error Screen

This error message screen displays until you press any key. Once the screen is acknowledged, IPL returns to the **Initial Program Loader** main menu to wait for a new selection.

To find the probable cause of the error, use the error number and/or the error text displayed on the screen to look up the error in [Table 7-4](#).

Table 7-4 *IPL Errors*

Error Text	Error Number	Probable Cause
Unknown error	-1	A general error occurred. Retry the download. If the failure persists, it is most likely due to a hardware failure; the wearable terminal requires servicing.
Cancelled by user	-2	The user canceled the download.
Can't open the source	-7	An error occurred opening the source device (either radio card or Serial port). Check source device connectivity and retry.
Can't open the destination	-8	An error occurred opening the destination device (either flash ROM or Power Micro). Retry the download. If the failure persists, it is most likely due to a hardware failure; the wearable terminal requires servicing.
Can't read from the source device	-9	The source device (either radio card or Serial port) could not be read from. Check source device connectivity and retry.
Can't write to the destination device	-10	The destination device (either flash ROM or Power Micro) could not be written to. Retry the download. If the failure persists, it is most likely due to a hardware failure; the wearable terminal requires servicing.
Transmission checksum error	-11	An error occurred during transmission from the source device (either radio card or Serial port) and the checksum check failed. Check source device connectivity and retry.
Readback checksum error	-12	A checksum, generated from reading back data that was written to the destination device, was incorrect. An error during transmission or a write error to the destination device could cause this.
There is no more heap space available	-14	There is no more heap space available for the download procedure. Restart IPL and retry the download. If the failure persists, contact service with details of what is being downloaded.
Insufficient data available to complete record	-21	A Symbol HEX file download was attempted but the HEX file is invalid. Ensure the file is in Symbol HEX file format.
Invalid Symbol HEX file	-23	A Symbol HEX file download was attempted but the HEX file is invalid. Ensure the file is in Symbol HEX file format.
Unrecognized or unsupported HEX record	-24	The Symbol HEX file being downloaded contains an invalid or unrecognized HEX record. Ensure the file is in proper Symbol HEX file format.
Invalid data in HEX file	-25	The Symbol HEX file being downloaded contains invalid data. Ensure the file is in proper Symbol HEX file format with valid HEX data.

Table 7-4 IPL Errors (Continued)

Error Text	Error Number	Probable Cause
Exceeded max size	-26	The download file is too large to fit into the space allocated for it. Either make the file smaller or increase the space allocated for it by altering the partition table.
Partition is not valid on this device	-27	The downloaded file specifies a partition entry that does not exist on the device. Only download files that are valid for this device, or change the partition table so that the new file is valid on the device.
Wrong destination code	-28	A specific partition was chosen from the Main Menu (not Auto Select) but the file selected for download was for another partition. Ensure that the partition selected from the Main Menu matches the file selected for download.
File type does not support IPL Auto Select	-29	Monitor, Power Micro and Partition Table cannot be loaded with Auto Select. Select the appropriate area, and try again.
Non-contiguous record found	-30	A Symbol HEX file download was attempted but the HEX file is invalid. Ensure the file is in Symbol HEX file format.
Timed Out - No data	-31	IPL was waiting for data from the source device but timed out before receiving any. Check the source device connectivity and retry.
Fail: Buffer Overrun	-32	The serial port device could not keep up with incoming data. Retry the serial download with a lower baud rate.
Partition Table not Valid	-33	The size of flash memory is different than that described in the partition table. Retry the download with the correct partition table file.
Invalid file format	-34	The file format is invalid. Only Symbol HEX files are supported by IPL.

Voice Only WT4090 IPL Error Indications

While downloading if there are any errors all three LEDs blink for three seconds and then turn solid.

Creating a Splash Screen

The source bitmap files used to create the default splash screens for the wearable terminal are supplied with the DCP for WT40x0c50. These files can be modified using any of the standard windows image editors, allowing customization for particular customers.

To create a custom splash screen, perform the following steps:

1. For wearable terminals with monochrome screens, open the Splashmono.bmp file supplied with the DCP for WT40x0c50 using an image editor.
2. For wearable terminals with color screens, open the Splashcolor.bmp file supplied with the DCP for WT40x0c50 using an image editor.
3. Modify the bitmap file and save.
4. Create a splash partition using the steps shown in the [Building the Image on page 7-9](#).
5. Splash Screen Format

If the default files are not used to create the new splash screens, be sure to preserve the image format. The formats are as follows:

Table 7-5 *Splash Screen Format*

Screen Type	Dimensions	Color Format
Color	320 x 216	8 bits per pixel*

* 8 bits per pixel only applies to splash screen images. Once Windows CE is running, the color density is 16 bits per pixel.

See [Sending the Hex Image Using IPL on page 7-11](#) for information about loading the splash screen using TCM and IPL.

Flash Storage

In addition to the RAM-based storage standard on Windows CE wearable terminals, the wearable terminal is also equipped with a non-volatile Flash-based storage area which can store data (partitions) that can not be corrupted by a cold boot. This Flash area is divided into two categories: Flash File System (FFS) Partitions and Non-FFS Partitions.

FFS Partitions

The wearable terminal includes two or three FFS partitions. These partitions appear to the wearable terminal as a hard drive that the OS file system can write files to and read files from. Data is retained even if power is removed.

The two or three FFS partitions appear as two or three separate folders in the Windows CE file system and are as follows:

- **Platform:** The Platform FFS partition contains Zebra-supplied programs and Dynamic Link Libraries (DLLs). This FFS is configured to include DLLs that control system operation. Since these drivers are required for basic wearable terminal operation, only experienced users should modify the content of this partition.
- **Application:** The Application FFS partition is used to store application programs needed to operate the wearable terminal.
- **On-Board IDE:** An additional 64 MB of FLASH memory available only on 128 MB/128 MB configurations. This partition can be used for additional application or data storage.

Working with FFS Partitions

Because the FFS partitions appear as folders under the Windows CE file system, they can be written to and read like any other folder. For example, an application program can write data to a file located in the Application folder just as it would to the Windows folder. However, the file in the Application folder is in non-volatile storage and is not lost on a cold boot (e.g., when power is removed for a long period of time).

Standard tools such as ActiveSync can be used to copy files to and from the FFS partitions. They appear as the "Application", "Platform" and "On-Board IDE" folders to the ActiveSync explorer. This is useful when installing applications on the wearable terminal. Applications stored in the Application folder are retained even when the wearable terminal is cold booted.

There are two device drivers included in the Windows CE image to assist developers in configuring the wearable terminal following a cold boot: RegMerge and CopyFiles.

RegMerge.dll

RegMerge.dll is a built-in driver that allows registry edits to be made to the Windows CE Registry. Regmerge.dll runs very early in the boot process and looks for registry files (.reg files) in certain Flash File System folders during a cold boot. It then merges the registry changes into the system registry located in RAM.

Since the registry is re-created on every cold boot from the default ROM image, the RegMerge driver is necessary to make registry modifications persistent over cold boots.

RegMerge is configured to look in the root of two specific folders for .reg files in the following order:

- \Platform
- \Application

Regmerge continues to look for .reg files in these folders until all folders are checked. This allows folders later in the list to override folders earlier in the list. This way, it is possible to override Registry changes made by the Platforms partitions folders. Take care when using Regmerge to make Registry changes. The DCP for WT4000c50 contains examples of .reg files.

✓ **NOTE** Regmerge only merges the .reg files on cold boots. The merge process is skipped during a warm boot.

Typically, do not make modifications to registry values for drivers loaded before RegMerge. However, these values may require modification during software development. Since these early loading drivers read these keys before RegMerge gets a chance to change them, the wearable terminal must be cold booted. The warm boot does not re-initialize the registry and the early loading driver reads the new registry values.

Do not use Regmerge to modify built-in driver registry values, or merge the same Registry value to two files in the same folder, as the results are undefined.

CopyFiles

Windows CE expects certain files to be in the Windows folder, residing in volatile storage. Windows CE maintains the System Registry in volatile storage. CopyFiles copies files from one folder to another on a cold boot. Files can be copied from a non-volatile partition (Application or Platform) to the Windows or other volatile partition during a cold boot. During a cold boot CopyFiles looks for files with a .CPY extension in the root of the Platform and Application FFS partitions (Platform first and then Application). These files are text files containing the source and destination for the desired files to be copied separated by ">". The following example from the file application.cpy is contained on the demo application partition included in the DCP for WT40x0c50. It can also be obtained from the Support Central web site at <http://www.zebra.com/support>.

Files are copied to the Windows folder from the Flash File System using copy files (*.cpy) in the following order:

- \Platform
- \Application

Example:

```
\Application\ScanSamp2.exe>\Windows\ScanSamp2.exe
```

This line directs CopyFiles to copy the ScanSamp2.exe application from the \Application folder to the \Windows folder.

Non-FFS Partitions

Non-FFS Partitions include additional software and data pre-loaded on the wearable terminal that can be upgraded. Unlike FFS Partitions, these partitions are not visible when the operating system is running. They also contain system information. Non-FFS partitions include the following:

- Windows CE: The complete Windows CE operating system is stored on Flash devices. If necessary, the entire OS image may be downloaded to the wearable terminal using files provided by Zebra. The current OS partition on the wearable terminal is included as part of the TCM installation package. Any upgrades must be obtained from Zebra. This partition is mandatory for the wearable terminal.
 - Splash Screen: a bitmap smaller than 16 kb (and limited to 8 bits per pixel) is displayed as the wearable terminal cold boots. To download a customized screen to display, see [Creating a Splash Screen on page 7-19](#).
- ✓ **NOTE** 8 bits per pixel only applies to splash screen images. Once Windows CE is running, the color density is 16 bits per pixel.
- IPL: This program interfaces with the host computer and allows downloading via cradle or serial cable any or all of the partitions listed above, as well as updated versions of IPL. Use caution downloading updated IPL versions; incorrect downloading of an IPL causes permanent damage to the wearable terminal. IPL is mandatory for the wearable terminal.
 - Partition Table: Identifies where each partition is loaded in the wearable terminal.

Downloading Partitions to the Wearable Terminal

TCM is used to specify a hex destination file for each partition and download each file to the wearable terminal. This download requires a program loader stored on the wearable terminal. The wearable terminal comes with a program loading utility, Initial Program Loader (IPL), stored in the wearable terminal's write-protected flash.

Chapter 8 Staging and Provisioning

Introduction

The MSP 3 Client Software is a set of software components that come pre-installed on the wearable terminal. The MSP 3 Client software consists of the following three components:

Refer to the Mobility Services Platform 3.2 User's Guide, p/n 72E-100158-06, for instructions for using the Rapid Deployment, AirBEAM Smart and MSP3 Agent clients.

Rapid Deployment (RD) Client

The RD Client provides support for MSP 3 Staging functionality, provides support for the MSP 3 Legacy Staging process, and provides support for backward-compatible legacy MSP 2.x Legacy Staging functionality.

AirBEAM Smart Client

The AirBEAM Smart Client provides backward-compatible legacy AirBEAM functionality and backward-compatible legacy MSP 2.x Level 2 Agent functionality.

MSP 3 Agent

The MSP 3 Agent provides MSP 3 Provisioning functionality and Control functionality when used with MSP 3.2 Control Edition.

Chapter 9 Special Considerations

Touch Panel User Interface Considerations

When developing applications for a touch panel interface, touch panel activation only by the ball of the finger means there are limitations to what the user interface of an application can expect of a worker

- User interface elements such as buttons, that require activation by a bare finger tip on the touch screen should not be smaller than 10 mm x 10 mm (as opposed to 5 mm x 5 mm if a stylus were an option).
- Do not put user interface elements close to the edge of the display. They're hard to activate and they might not be fully covered by the protective overlay. Keep the touch points at least 2 mm in from the edge.

Tips for Improving Battery Life

To improve the life of the battery:

- Set the display backlight to turn off quickly and reduce the display brightness.
- Set the keypad backlight to turn off quickly.
- Set the wearable computer to suspend when not in use and maximum CPU performance.
- Set the WLAN radio to save maximum power.

After making these settings, they can be saved in Registry files to make them cold-boot persistent.

Display Backlight



NOTE Changing the Backlight setting on the Voice Only WT4090 will change the brightness of the Application Controlled LED. Refer to the EMDK Help file WT4090-VOW Programming page for more information.

To change the display backlight settings in order to conserve battery power:

1. Select **Start > Settings > Control Panel**.
2. Select **Backlight** icon.
3. Select **Battery Power** tab.

4. Ensure that the **Disable backlight if not used for** checkbox is checked.
5. In the drop-down list, select the amount of time after which the display will turn off. Set to **1 minute** or a lower value that the user is comfortable with.

To set the brightness level of the display:

1. Select **Brightness** tab.
2. Move the slider to **2** to conserve power.
3. Select **OK**.

Keypad Light



NOTE Changing the Keypad Backlight setting on the Voice Only WT4090 will change the brightness of the WLAN Status LED. Refer to the EMDK Help file WT4090-VOW Programming page for more information.

To set the amount of time that the keypad light stays on:

1. Select **Start > Settings > Control Panel**.
2. Select **Keylight** icon.
3. Select **Battery Power** tab.
4. Ensure that the **Disable keylight if not used for** checkbox is checked.
5. In the drop-down list, select the amount of time after which the keypad light will turn off. Set to **1 minute** or a lower value that the user is comfortable with.

To disable the key light from coming on:

1. Select the **Advanced** tab.
2. Ensure that the **Disable keylight** checkbox is checked.

Tap **OK**.

Power

To set the wearable computer to turn off after a short period of non-use:

1. Select **Start > Settings > Control Panel**.
2. Select **Power** icon.
3. Select **Power Off** tab
4. Ensure that the **Turn off device if not used for** checkbox is checked
5. In the drop-down list, select the amount of time after which the device will turn off. The default setting is 3. If desired, lower this value to 1 to conserve power.

To set the CPU to maximum performance:

1. Select **CPU Power** tab.
2. Ensure that the **Max. Performance** radio button is selected. This selection maximizes battery life.
3. Select **Apply**.

4. Select **OK**.

Wireless LAN

To set the WLAN radio to maximum performance:

1. Select the wireless icon in the bottom lower right corner.
2. Select **Manage Profiles**.
3. Select your wireless profile, double click.
4. Select **Edit**.
5. Continuously select **Next** until the **Battery Usage** window appears.
6. Ensure the **MAX Power Save** radio button is selected.

Voice Only WT4090 LED Considerations

- Application developers for the Voice Only WT4090 should not program all LEDs to be turned on at the same time, as this sequence is reserved for IPL mode.
- Do not turn off the display backlight or the keypad backlight as this will turn off the Application Controlled LED and the WLAN Status LED, respectively.
- Consider device battery life when programming LED blinking. Refer to the EMDK Help file WT4090-VOW Programming page for more information.

Chapter 10 Maintenance & Troubleshooting

Introduction

This chapter includes instructions on cleaning and storing the wearable terminal, and provides troubleshooting solutions for potential problems during wearable terminal operating.

Maintaining the Wearable Terminal

For trouble-free service, observe the following tips when using the wearable computer:

- Do not scratch the touch screen of the wearable computer. When activating with the wearable computer touch screen, use finger tips. Never use a pen or pencil or other sharp object on the surface of the screen.

Zebra requires using a screen protector, p/n KT-114032-01R or KT-114032-02R.

- A screen protector is applied to the wearable computer touch screen. Zebra requires using this to minimize wear and tear. Screen protectors enhance the usability and durability of touch screen displays. Benefits include:
 - Protection from scratches and gouges
 - Durable touch surface with tactile feel
 - Abrasion and chemical resistance
 - Keeping the device's screen looking new
 - Quick and easy installation.
- Protect the wearable computer with a touch screen from temperature extremes.
- Do not store or use the wearable computer with a touch screen in any location that is extremely dusty, damp, or wet.
- Use a soft lens cloth to clean the wearable computer display/touch screen.
- Periodically replace the rechargeable Li-ion battery to ensure maximum battery life and product performance. Battery life depends on individual usage patterns.
- The screen of the wearable computer contains glass. Take care not to drop the wearable computer or subject it to strong impact.

- Regularly replace all Velcro® straps on the wrist mount and wearable scanners, to ensure adequate adhesion of the Velcro.
- On touch screen versions, periodically replace the screen protector, especially if it is scratched.

Wrist Mount Cleaning Instructions

It may be necessary to wash the wrist mount straps and replaceable pad when they become soiled.

Remove the straps and pad from the wrist mount. Hand wash in cold water with a mild detergent (such as Woolite®). Do not use bleach. Air dry. Do not use a dryer.

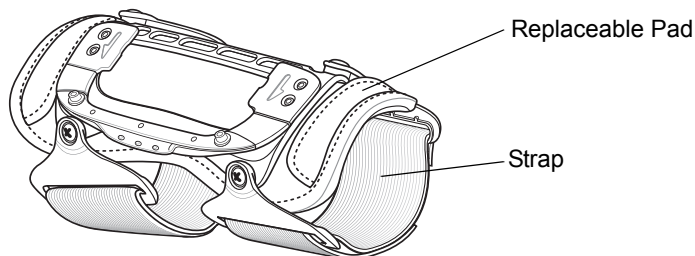


Figure 10-1 Wrist Mount Soft Goods

Arm Sleeve Cleaning Instructions

It may be necessary to wash the arm sleeve when it become soiled.

Hand wash in cold water with a mild detergent (such as Woolite®). Do not use bleach. Air dry. Do not use a dryer.

Removing the Screen Protector

- ✓ **NOTE** Not using a screen protector on a touch panel device can affect warranty coverage. To purchase replacement protectors, contact your local account manager or Zebra. These include screen protector installation instructions. Part number: KT-67525-01R or KT-67525-02R Screen Protector 3/pk.

A screen protector is applied to the wearable terminal with touch screen. Zebra mandates using this to minimize wear and tear. Screen protectors enhance the usability and durability of touch screen displays.

To remove the screen protector, lift the corner using a thin plastic card, such as a credit card, then carefully lift it off the display.

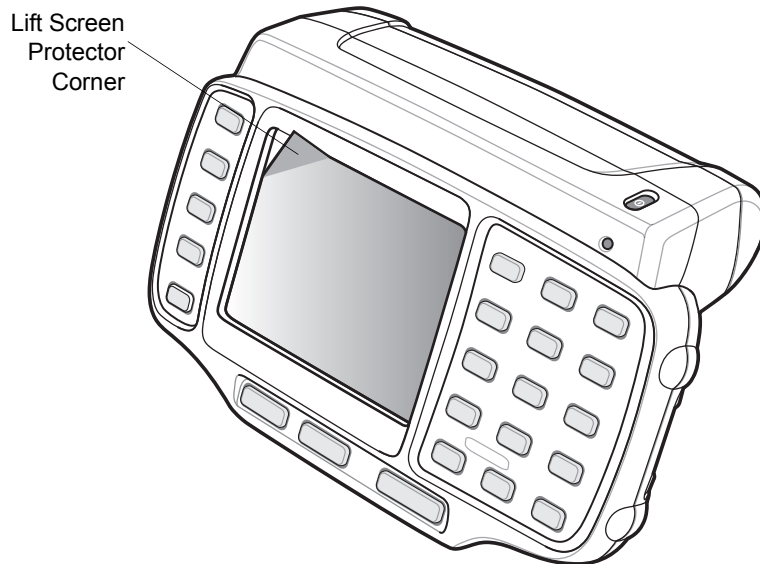


Figure 10-2 *Removing the Screen Protector*



CAUTION Do not use a sharp object to remove the protector. Doing so can damage the touch screen.

Battery Safety Guidelines

- The area in which the units are charged should be clear of debris and combustible materials or chemicals. Particular care should be taken where the device is charged in a non commercial environment.
- Improper battery use may result in a fire, explosion, or other hazard.
- To charge the mobile device battery, the battery and charger temperatures must be between 0 °C and +40 °C (+32 °F and +104 °F).
- Do not use incompatible batteries and chargers. Use of an incompatible battery or charger may present a risk of fire, explosion, leakage, or other hazard. If you have any questions about the compatibility of a battery or a charger, contact Zebra support.
- Do not disassemble or open, crush, bend or deform, puncture, or shred.
- Severe impact from dropping any battery-operated device on a hard surface could cause the battery to overheat.
- Do not short circuit a battery or allow metallic or conductive objects to contact the battery terminals.
- Do not modify or remanufacture, attempt to insert foreign objects into the battery, immerse or expose to water or other liquids, or expose to fire, explosion, or other hazard.
- Do not leave or store the equipment in or near areas that might get very hot, such as in a parked vehicle or near a radiator or other heat source. Do not place battery into a microwave oven or dryer.
- Battery usage by children should be supervised.
- Please follow local regulations to promptly dispose of used re-chargeable batteries.
- Do not dispose of batteries in fire.

- Seek medical advice immediately if a battery has been swallowed.
- In the event of a battery leak, do not allow the liquid to come in contact with the skin or eyes. If contact has been made, wash the affected area with large amounts of water and seek medical advice.
- If you suspect damage to your equipment or battery, contact Zebra support to arrange for inspection.

Cleaning



WARNING! Avoid exposing this product to contact with hot oil or other flammable liquids. If such exposure occurs, unplug the device and clean the product immediately in accordance with these guidelines.



CAUTION Always wear eye protection.

Read warning label on compressed air and alcohol product before using.

If you have to use any other solution for medical reasons please contact Zebra for more information.

Materials Required

- Alcohol wipes
- Soft lens cloth
- Cotton tipped applicators
- Isopropyl alcohol
- Can of compressed air with a tube.

Cleaning the Wearable Terminal

Housing

Using the alcohol wipes, wipe the housing including keys and in-between keys.

Display

The display can be wiped down with the alcohol wipes, but care should be taken not to allow any pooling of liquid around the edges of the display. Immediately dried the display with a soft, non-abrasive cloth to prevent streaking. For WT4090 with touch panel, only use a soft lens cloth to clean the touch panel overlay surface.

Connectors

Clean all three connectors, two interface connectors on the sides of the wearable terminal and the cradle connector on the back.

1. Remove the main battery from mobile computer. See [Installing the Main Battery on page 1-4](#).
2. Remove connector rubber plugs, if required.
3. Dip the cotton portion of the cotton tipped applicator in isopropyl alcohol.

4. Rub the cotton portion of the cotton tipped applicator back-and-forth across each connector. Do not leave any cotton residue on the connector.
5. Repeat at least three times.
6. Use the cotton tipped applicator dipped in alcohol to remove any grease and dirt near the connector area.
7. Use a dry cotton tipped applicator and repeat steps 4 through 7.



CAUTION Do not point nozzle at yourself and others, ensure the nozzle or tube is away from your face.

8. Spray compressed air on the connector areas by pointing the tube/nozzle about ½ inch away from the surface.
9. Inspect the area for any grease or dirt, repeat if required.
10. Replace connector rubber plugs, if required.

Cleaning the RS309, RS409 and RS507

Housing

Using the alcohol wipes, wipe the housing including keys and in-between keys.

Scanner Exit Window

Wipe the scanner exit window periodically with a lens cloth or other material suitable for cleaning optical material such as eyeglasses.

Connectors

1. Disconnect the scanner from mobile computer.
2. Dip the cotton portion of the cotton tipped applicator in isopropyl alcohol.
3. Rub the cotton portion of the cotton tipped applicator back-and-forth across the connector pins. Do not leave any cotton residue on the connector.
4. Repeat at least three times.
5. Use the cotton tipped applicator dipped in alcohol to remove any grease and dirt near the connector area. Use a dry cotton tipped applicator and repeat steps 3 through 5.



CAUTION Do not point nozzle at yourself and others, ensure the nozzle or tube is away from your face.

6. Spray compressed air on the connector area by pointing the tube/nozzle about ½ inch away from the surface.
7. Inspect the area for any grease or dirt, repeat if required.

Cleaning Cradle Connectors

To clean the connectors on a cradle:

1. Remove the DC power cable from the cradle.
2. Dip the cotton portion of the cotton tipped applicator in isopropyl alcohol.

3. Rub the cotton portion of the cotton tipped applicator along the pins of the connector. Slowly move the applicator back-and-forth from one side of the connector to the other. Do not let any cotton residue on the connector.
4. All sides of the connector should also be rubbed with the cotton tipped applicator.



CAUTION Do not point nozzle at yourself and others, ensure the nozzle or tube is away from your face.

5. Spray compressed air in the connector area by pointing the tube/nozzle about ½ inch away from the surface.
6. Ensure that there is no lint left by the cotton tipped applicator, remove lint if found.
7. If grease and other dirt can be found on other areas of the cradle, use lint free cloth and alcohol to remove.



8. Allow at least 10 to 30 minutes (depending on ambient temperature and humidity) for the alcohol to air dry before applying power to cradle.

If the temperature is low and humidity is high, longer drying time is required. Warm temperature and dry humidity requires less drying time.

Cleaning Frequency

The cleaning frequency is up to the customer's discretion due to the varied environments in which the mobile devices are used. They may be cleaned as frequently as required. However when used in dirty environments it may be advisable to periodically clean the ring scanners' exit windows to ensure optimum scanning performance.

Troubleshooting

Wearable Terminal

Table 10-1 *Troubleshooting the Wearable Terminal*

Problem	Cause	Solution
Wearable terminal does not turn on.	Lithium-ion battery not charged.	Charge or replace the lithium-ion battery in the wearable terminal.
	Lithium-ion battery not installed properly.	Ensure battery is installed properly. See Installing and Removing the Main Battery on page 1-4 .
	System crash.	Perform a warm boot. If the wearable terminal still does not turn on, perform a cold boot. See Resetting the Wearable Terminal on page 1-8 .

Table 10-1 *Troubleshooting the Wearable Terminal (Continued)*

Problem	Cause	Solution
Rechargeable lithium-ion battery did not charge.	Battery failed.	Replace battery. If the wearable terminal still does not operate, try a warm boot, then a cold boot. See Resetting the Wearable Terminal on page 1-8 .
	Wearable terminal removed from cradle while battery was charging.	Insert wearable terminal in cradle and begin charging.
	Ambient temperature of the cradle is too warm or too cold.	Move the cradle to an area where the ambient temperature is between 0 °C and 40 °C (32 °F and 104 °F).
Cannot see characters on display (not applicable to voice only configuration).	Wearable terminal not powered on.	Press the Power button.
Display on touch panel version is hard to read (not applicable to voice only configuration).	Screen protector may be scratched or worn.	Replace screen protector.
During data communication, no data was transmitted, or transmitted data was incomplete.	Wearable terminal removed from cradle or unplugged from host computer during communication.	Replace the wearable terminal in the cradle, or reattach the Synchronization cable and re-transmit.
	Incorrect cable configuration.	See the System Administrator.
	Communication software was incorrectly installed or configured.	Perform setup. See Chapter 2, Accessories for details. Ensure that Microsoft ActiveSync 4.1 or greater is installed on the host computer.
No sound is audible.	Volume setting is low or turned off.	Adjust volume. Change volume settings by selecting Start > Settings > Control Panel > Volume & Sounds icon > Volume tab. Move the slider to change the volume level or use volume control on voice application.

Table 10-1 *Troubleshooting the Wearable Terminal (Continued)*

Problem	Cause	Solution
Wearable terminal turns itself off.	Wearable terminal is inactive.	The wearable terminal turns off after a period of inactivity. If the wearable terminal is running on battery power, this period can be set to 30 sec., 1, 2, 3, 4, 5 or 6 minutes. If the wearable terminal is running on external power, this period can be set to 1, 2, 3, 5, 10, 15 and 30 minutes. Check the power settings by selecting Start > Settings > Control Panel > Power icon > Power Off tab. Change the setting if you need a longer delay before the automatic shutoff feature activates.
	Voice Only WT4090 was set to suspend.	Return Voice Only WT4090 suspend setting to factory default (disabled).
	Battery is depleted.	Replace or recharge the battery.
	Battery is not inserted properly.	Insert the battery properly (see Installing and Removing the Main Battery on page 1-4).
	The wearable computer's battery is low and it powers down to protect memory content.	Replace or recharge the battery.
A message appears stating that the wearable terminal memory is full. (not applicable to voice only configuration).	Too many files stored on the wearable terminal.	Delete unused memos and records. You can save these records on the host computer.
	Too many applications installed on the wearable terminal.	If you have installed additional applications on the wearable terminal, remove them to recover memory. Select Start > Settings > Control Panel > Remove Programs icon. Select the unused program and select Remove .

Table 10-1 *Troubleshooting the Wearable Terminal (Continued)*

Problem	Cause	Solution
The wearable terminal does not accept scan input.	Scanning application is not loaded.	Verify that the unit is loaded with a scanning application. See the System Administrator.
	Unreadable bar code.	Ensure the symbol is not defaced.
	Distance between exit window and bar code is incorrect.	Ensure wearable terminal is within proper scanning range.
	Wearable terminal is not programmed for the bar code.	Ensure the wearable terminal is programmed to accept the type of bar code being scanned.
	Wearable terminal is not programmed to generate a beep.	If a beep on a good decode is expected and a beep is not heard, check that the application is set to generate a beep on good decode.
	Battery is low.	If the scanner stops emitting a laser beam when the trigger is pressed, check the battery level. When the battery is low, the scanner shuts off before the wearable terminal low battery condition notification. Note: If the scanner is still not reading symbols, contact the distributor or Zebra.
Wearable terminal goes into IPL mode after cold boot.	Headset adapter without a headset is connected to the wearable terminal during a cold boot.	Disconnect the headset adapter prior to performing a cold boot.
	Scanner trigger is held down during a cold boot.	Do not press trigger during a cold boot.
	P1 or P2 key is held down during a cold boot.	Do not press the P1 or P2 key during a cold boot.
If all three LEDs are lit solid.	Voice Only WT4090 is in IPL mode.	Perform cold boot. See Resetting the Wearable Terminal on page 1-8 .
WLAN connection is lost when the wearable terminal is connected to a host computer using ActiveSync.	Microsoft security feature prevents connection to two separate networks.	Disconnect from the WLAN network prior to connecting to a host computer using ActiveSync.

Four Slot Spare Battery Charger

Table 10-2 *Troubleshooting The Four Slot Spare Battery Charger*

Symptom	Possible Cause	Solution
Batteries not charging.	Battery was removed from the charger or charger was unplugged from AC power too soon.	Re-insert the battery in the charger or re-connect the charger's power supply.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	Battery contacts not connected to charger.	Verify that the battery is seated in the battery well correctly with the contacts facing down.
	Ambient temperature of the charger is too warm or too cold.	Move the charger to an area where the ambient temperature is between 0 °C and 40 °C.

Four Slot Ethernet Cradle

Table 10-3 *Troubleshooting the Four Slot Ethernet Cradle*

Problem	Cause	Solution
Wearable terminal amber Charge Status LED does not light when wearable terminal inserted.	Cradle is not receiving power.	Ensure the power cable is connected securely to both the cradle and to AC power.
	Wearable terminal is not correctly seated.	Remove and re-insert the wearable terminal into the cradle, ensuring it is correctly seated.
Wearable terminal battery is not charging.	Wearable terminal was removed from cradle or cradle was unplugged from AC power too soon.	Ensure cradle is receiving power. Ensure the wearable terminal is seated correctly.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	The wearable terminal is not fully seated in the cradle.	Remove and re-insert the wearable terminal into the cradle, ensuring it is correctly seated.
	Ambient temperature of the cradle is too warm or too cold.	Move the cradle to an area where the ambient temperature is between 0 °C and 40 °C (32 °F and 104 °F).

Table 10-3 Troubleshooting the Four Slot Ethernet Cradle (Continued)

Problem	Cause	Solution
During data communication, no data was transmitted, or transmitted data was incomplete.	Wearable terminal removed from cradle during communication.	Replace wearable terminal in cradle and retransmit.
	Incorrect cable configuration.	See the system administrator.
	Ethernet connection error. Link LED is not lit (see Link LED on page 2-10).	See the system administrator. Probable Ethernet connection error.

Single Slot USB Cradle

Table 10-4 Troubleshooting the Single Slot USB Cradle

Symptom	Possible Cause	Action
LEDs do not light when wearable terminal or spare battery is inserted.	Cradle is not receiving power.	Ensure the power cable is connected securely to both the cradle and to AC power.
	Wearable terminal is not seated firmly in the cradle.	Remove and re-insert the wearable terminal into the cradle, ensuring it is firmly seated.
	Spare battery is not seated firmly in the cradle.	Remove and re-insert the spare battery into the charging slot, ensuring it is firmly seated.
Wearable terminal battery is not charging.	Wearable terminal was removed from cradle or cradle was unplugged from AC power too soon.	Ensure cradle is receiving power. Ensure wearable terminal is seated correctly. Confirm main battery is charging. View battery status by selecting Start > Settings > Control Panel > Power icon.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	The wearable terminal is not fully seated in the cradle.	Remove and re-insert the wearable terminal into the cradle, ensuring it is firmly seated.
	Ambient temperature of the cradle is too warm or too cold.	Move the cradle to an area where the ambient temperature is between 0 °C and 40 °C (32 °F and 104 °F).
Spare battery is not charging.	Battery not fully seated in charging slot.	Remove and re-insert the spare battery into the cradle, ensuring it is firmly seated.
	Battery inserted incorrectly.	Ensure the contacts are facing down and toward the back of the cradle.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.

Table 10-4 Troubleshooting the Single Slot USB Cradle (Continued)

Symptom	Possible Cause	Action
During data communications, no data was transmitted, or transmitted data was incomplete.	Wearable terminal removed from cradle during communications.	Replace wearable terminal in cradle and retransmit.
	Incorrect cable configuration.	See the System Administrator.
	Communications software is not installed or configured properly.	Perform setup as described in Chapter 2, Accessories . Ensure that Microsoft ActiveSync 4.1 or greater is installed on the host computer.
Cannot ActiveSync with Host Computer	Wrong USB cable used.	Ensure that the cable has a USB A connector on one end and a USB mini B connector on the other end.
	Host computer not configured properly.	Ensure that ActiveSync on the host computer is set to allow USB connections.
	The wearable computer is not fully seated in the cradle.	Remove and re-insert the wearable computer into the cradle, ensuring it is firmly seated.

Appendix A Technical Specifications

Technical Specifications

The following tables summarize the wearable terminal's intended operating environment and general technical hardware specifications.

Wearable Terminal

The following table summarizes the wearable terminal's intended operating environment.

Table A-1 *Technical Specifications*

Item	Description
Physical and Environmental Characteristics	
Dimensions	With Standard Battery: 5.7 inches L x 3.7 inches W x 1.0 inch H (14.2 cm L x 9.3 cm H x 2.6 cm H) With Extended Battery: 5.7 inches L x 4.2 inches W x 1.0 inch H (14.2 cm L x 10.7 cm H x 2.6 cm H)
Weight (including battery)	With Standard Battery: 11.3 oz. (320 g) With Extended Battery: 12.2 oz. (345 g)
Keyboard	WT4070/90: Two-color Alphanumeric Keypad or Triple-tap Alphanumeric Keypad Voice Only WT4090: Three programmable function keys.
Display	WT4070/90: Color 2.8 inch QVGA non-touch or touch screens Voice Only WT4090: None
Main Battery	Removable, rechargeable 3.7 VDC Lithium Ion battery. Standard capacity: 2330 mAh (minimum) Extended capacity: 4600 mAh (minimum)
Backup Battery	NiMH battery (rechargeable) 15 mAh 2.4 VDC (not user accessible)
Performance Characteristics	
CPU	XScale PXA270 processor at 520 MHz

Table A-1 *Technical Specifications (Continued)*

Item	Description
Operating System	Microsoft Windows CE 5.0 Professional
Memory	64 MB Flash/128 MB RAM or 128 MB Flash/128 MB RAM
Application Development	PSDK, DCP and SMDK available through Zebra Developer Zone web site
Data Capture Options	RS309 scanner RS409 scanner RS507 Hands-free Imager
User Environment	
Operating Temperature	-4 °F to 122°F (-20 °C to 50 °C)
Storage Temperature	-40 °F to 158 °F (-40 °C to 70 °C)
Battery Charging Temperature	32 °F to 104 °F (0 °C to +40 °C) ambient temperature range.
Humidity	5% to 95% non condensing
Drop Specification	Multiple 4 ft.(1.2 m) drops to concrete across operating temperature range
Tumble	500 half-meter tumbles at room temperature (1,000 drops)
Environmental Sealing	IP54 Category 2
ESD	± 15k VDC air discharge ± 8k VDC direct discharge ± 8k VDC indirect discharge
WLAN Wireless Data Communications	
WLAN radio	WT4070: Zebra 802.11b/g WT4090: Zebra 802.11a/b/g
Operating Channels	Channel 8 - 169 (5040 - 5845 MHz) (4920 - 4980 MHz) Japan only Channel 1 - 13 (2412 - 2472 MHz) Channel 14 (2484 MHz) Japan only Actual operating frequencies depend on regulatory rules and certification agency
Security	WEP2 (40 or 128 bit), TKIP, TLS, TTLS (MS-CHAP), TTLS (MS-CHAP v2), TTLS (CHAP), TTLS-MD5, TTLS-PAP, PEAP-TLS, PEAP (MS-CHAP v2), AES, LEAP, CCX v3
Voice Communication	Runs voice recognition engines and text-to-speech engines for voice picking applications
Output Power	100 mW U.S. and International
Data Rate	802.11a: up to 54Mb per second 802.11b: up to 11Mb per second 802.11g: up to 54Mb per second
Frequency Range	802.11a: 5 GHz; country-dependent 802.11b: 2.4 GHz; country-dependent 802.11g: 2.4 GHz; country-dependent

Table A-1 *Technical Specifications (Continued)*

Item	Description
Antenna	Internal
WPAN Wireless Data Communications	
Bluetooth	Bluetooth Version 1.2

Table A-1 *Technical Specifications (Continued)*

Item	Description
Peripherals and Accessories	
Cradles	Single Slot USB Four Slot Ethernet
Printers	Supports extensive line of Zebra approved printers, cables and accessories
Charger	Four Slot Battery Charger
Other Accessories	Headset adapter, freezer pouch, hip mount and wrist mount.
Regulatory	
Electrical Safety	Certified to UL60950-1, CSA C22.2 No. 60950-1, EN60950/IEC 60950-1 plus all national deviations
EMC	FCC Part 15 Subpart B, ICES-003 Class B, EN 60601-1-2, EN 61000-3-2, EN 61000-3-3, CISPR 22 Class B, CISPR 24
RF	FCC Parts 15.247, 15.407, 15.205, 15.207, 15.209, 15.203, EN 300 32, EN301 893, RSS-100, RSS-210, ARIB STD-66 & 33, ARIB STD-T70 & 71

RS309 Scanner

Table A-2 *RS309 Technical Specifications*

Item	Description																												
Physical and Environmental Characteristics																													
Dimensions (standard version without cables attached)	2.7 inch L x 2.4 inch W x 1.5 inch H (6.8 cm L x 6.1 cm H x 3.8 cm)																												
Weight (standard version without cables attached)	3.525 oz. (98 gm)																												
Current	140 mA typical, 180 mA max																												
Standby Current	60 μ A max																												
Voltage	3.1 to 3.6 VDC																												
Vcc Noise Level	200 mV p-p max.																												
Performance Characteristics																													
Light Source	650 nm LASER, 1.06 mW																												
Scan Rate	35 (\pm 5) scans/sec (bidirectional)																												
Nominal Working Distance	<table border="0"> <tr> <td>Density</td> <td>5 mil</td> <td>7.5 mil</td> <td>13 mil</td> <td>20 mil</td> <td>55 mil</td> <td></td> </tr> <tr> <td>Code Type</td> <td>39</td> <td>39</td> <td>UPC</td> <td>39</td> <td>39</td> <td></td> </tr> <tr> <td>Far (inches)</td> <td>7</td> <td>9.75</td> <td>20.25</td> <td>29.25</td> <td>54.5</td> <td>(Guaranteed)</td> </tr> <tr> <td>Far (inches)</td> <td>9.5</td> <td>15.25</td> <td>27.25</td> <td>42.5</td> <td>84.75</td> <td>(Typical)</td> </tr> </table>	Density	5 mil	7.5 mil	13 mil	20 mil	55 mil		Code Type	39	39	UPC	39	39		Far (inches)	7	9.75	20.25	29.25	54.5	(Guaranteed)	Far (inches)	9.5	15.25	27.25	42.5	84.75	(Typical)
Density	5 mil	7.5 mil	13 mil	20 mil	55 mil																								
Code Type	39	39	UPC	39	39																								
Far (inches)	7	9.75	20.25	29.25	54.5	(Guaranteed)																							
Far (inches)	9.5	15.25	27.25	42.5	84.75	(Typical)																							
Yaw	\pm 50 degrees from normal																												
Roll	\pm 20 degrees from vertical																												

Table A-2 RS309 Technical Specifications (Continued)

Item	Description																		
Pitch	± 65 degrees from normal																		
User Environment																			
Operating Temperature	-22 °F to 122 °F (-30 °C to 50 °C)																		
Storage Temperature	-40 °F to 140 °F (-40 °C to 60 °C)																		
Humidity	5% to 95% non condensing																		
Drop Specification	4 ft.(1.8m) drop to concrete																		
Environmental Sealing	IP54 sealing																		
Ambient Light Immunity	Indoor: 450 foot-candles (4,844 lux) Outdoor: 8,000 foot-candles (86,111 lux)																		
Regulatory																			
Electrical Safety	Certified to CSA C22.2 No. 60950-1, EN60950-1, IEC 60950-1																		
EMI/RFI	FCC Part 15 Class B, ICES-003 Class B, European Union EMC and R&TTE Directives, Australian AS/NZS 4268																		
Laser Safety	CDRH Class II, IEC 60825-1 Class 2																		
Laser Decode Capability	<table border="0"> <tr> <td>Code 39</td> <td>Code 128</td> <td>Code 93</td> </tr> <tr> <td>Codabar</td> <td>Code 11</td> <td>Discrete 2 of 5</td> </tr> <tr> <td>Interleaved 2 of 5</td> <td>EAN-8</td> <td>EAN-13</td> </tr> <tr> <td>MSI</td> <td>UPCA</td> <td>UPCE</td> </tr> <tr> <td>UPC/EAN supplementals</td> <td>Coupon Code</td> <td>Trioptic 39</td> </tr> <tr> <td>Webcode</td> <td>Chinese 2 of 5</td> <td>RSS</td> </tr> </table>	Code 39	Code 128	Code 93	Codabar	Code 11	Discrete 2 of 5	Interleaved 2 of 5	EAN-8	EAN-13	MSI	UPCA	UPCE	UPC/EAN supplementals	Coupon Code	Trioptic 39	Webcode	Chinese 2 of 5	RSS
Code 39	Code 128	Code 93																	
Codabar	Code 11	Discrete 2 of 5																	
Interleaved 2 of 5	EAN-8	EAN-13																	
MSI	UPCA	UPCE																	
UPC/EAN supplementals	Coupon Code	Trioptic 39																	
Webcode	Chinese 2 of 5	RSS																	

RS409 Scanner

Table A-3 RS409 Technical Specifications

Item	Description
Physical and Environmental Characteristics	
Dimensions	1.9 in. L x 1.4 in. W x 1.9 in. H (4.8 cm L x 3.6 cm H x 4.8 cm H)
Weight (standard version without cables attached)	2.0 oz. (56.7 gm)
Current	92 mA typical, 121 mA max
Standby Current	12µA typical/60 µA max
Voltage	3.1 to 3.6 VDC
Vcc Noise Level	100 mV p-p max.
Performance Characteristics	
Light Source	650 nm LASER, 1.55 mW

Table A-3 RS409 Technical Specifications (Continued)

Item	Description							
Scan Rate	104 (± 12) scans/sec (bidirectional)							
Nominal Working Distance	Density	5 mil	7.5 mil	10 mil	13 mil	20 mil	40 mil	55 mil
	Code Type	39	39	39	UPC	39	39	39
	Far (inches)	4.75	8.75	13.25	17.25	21.5	22.25	27 (Guaranteed)
	Far (inches)	8.75	14.25		24.25	35.75		50.5 (Typical)
Yaw	± 50 degrees from normal							
Roll	± 35 degrees from vertical							
Pitch	± 65 degrees from normal							
User Environment								
Operating Temperature	-4 °F to 122 °F (-20 °C to 50 °C)							
Storage Temperature	-25 °F to 160 °F (-40 °C to 70 °C)							
Humidity	5% to 95% non condensing							
Drop Specification	4 ft.(1.8m) drop to concrete							
Environmental Sealing	IP54 sealing							
Ambient Light Immunity	Indoor: 450 foot-candles (4,844 lux) Outdoor: 8,000 foot-candles (86,111 lux)							
Regulatory								
Electrical Safety	Certified to CSA C22.2 No. 60950-1, EN60950-1, IEC 60950-1							
EMI/RFI	FCC Part 15 Class B, ICES-003 Class B, European Union EMC and R&TTE Directives, Australian AS/NZS 4268							
Laser Safety	CDRH Class II, IEC 60825-1 Class 2							
Laser Decode Capability	Code 39			Code 128			Code 93	
	Codabar			Code 11			Discrete 2 of 5	
	Interleaved 2 of 5			EAN-8			EAN-13	
	MSI			UPCA			UPCE	
	UPC/EAN supplementals			Coupon Code			Trioptic 39	
	Webcode			Chinese 2 of 5			RSS	

RS507 Scanner

Table A-4 RS507 Technical Specifications

Item	Description																																								
Physical and Environmental Characteristics																																									
Dimensions	Triggerless, standard battery: 2.9 x 5.3 x 7.4 cm (1.16 x 2.1 x 2.92 in.) Triggerless, extended battery: 3.6 x 5.3 x 7.4 cm (1.42 x 2.1 x 2.92 in.) Triggered, standard battery: 2.9 x 5.3 x 7.4 cm (1.16 x 2.1 x 2.92 in.) Triggered, corded (cord length not included): 3.3 x 5.3 x 7.4 cm (1.3 x 2.1 x 2.92 in.)																																								
Weight	Triggerless, standard battery: 121.4 g (4.3 oz.) Triggerless, extended battery: 146.4 g (5.2 oz.) Triggered, standard battery: 134.8 g (4.8 oz.) Triggered, corded: 140.8 g (5.0 oz.)																																								
Performance Characteristics																																									
Optical Resolution	WVGA 752 H x 480 V pixels (gray scale)																																								
Skew	± 60° from normal																																								
Roll	360°																																								
Pitch	± 60° from normal																																								
Aiming Element	655 nm ± 10 nm Visible Laser Diode																																								
Illumination Element	637 nm ± 5 nm Red LEDs																																								
Field of View	Horizontal: 39.6°; Vertical: 25.7°																																								
Nominal Working Distance	<table border="0"> <tr> <td>Density</td> <td>5 mil</td> <td>7.5 mil</td> <td>20 mil</td> <td>13 mil</td> </tr> <tr> <td>1D Code Type</td> <td>39</td> <td>39</td> <td>39</td> <td>UPC</td> </tr> <tr> <td>Near</td> <td>2"</td> <td></td> <td></td> <td>1.5"</td> </tr> <tr> <td>Far</td> <td>7.4"</td> <td>10.5"</td> <td>24.6"</td> <td>15.4"</td> </tr> <tr> <td>Density</td> <td>6.67 mil</td> <td>10 mil</td> <td>15 mil</td> <td></td> </tr> <tr> <td>2D Code Type</td> <td>PDF417</td> <td>PDF417</td> <td>PDF417</td> <td></td> </tr> <tr> <td>Near</td> <td>3.3"</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Far</td> <td>7.0"</td> <td>10"</td> <td>14.6"</td> <td></td> </tr> </table>	Density	5 mil	7.5 mil	20 mil	13 mil	1D Code Type	39	39	39	UPC	Near	2"			1.5"	Far	7.4"	10.5"	24.6"	15.4"	Density	6.67 mil	10 mil	15 mil		2D Code Type	PDF417	PDF417	PDF417		Near	3.3"				Far	7.0"	10"	14.6"	
Density	5 mil	7.5 mil	20 mil	13 mil																																					
1D Code Type	39	39	39	UPC																																					
Near	2"			1.5"																																					
Far	7.4"	10.5"	24.6"	15.4"																																					
Density	6.67 mil	10 mil	15 mil																																						
2D Code Type	PDF417	PDF417	PDF417																																						
Near	3.3"																																								
Far	7.0"	10"	14.6"																																						
Ambient Light Immunity	From total darkness Indoor: 450 ft. candles (4,845 lux). Outdoor: 9,000 ft. candles (96,900 lux).																																								
Motion Tolerance	63.5 cm (25 inches) per second, typical.																																								

Table A-4 RS507 Technical Specifications (Continued)

Item	Description
Supported Symbologies	<p>1D enabled by default: Codabar, Code 39, Code 128, EAN-13, EAN-8, Interleaved 2 of 5, UPC-A and UPC-E.</p> <p>Additionally supported by 1D: Code 11, Code 32 Pharmaceutical (PARAF), Code 93, MSI, Reduced Space Symbology (RSS-14, RSS Limited, RSS Expanded), Straight 2 of 5 IATA (two-bar start/stop), Straight 2 of 5 Industrial (three-bar start/stop), Trioptic, UPC-E1.</p> <p>2D enabled by default: 4-CB (4-State Customer Bar code), Aztec, MicroPDF417, PDF417, MaxiCode.</p> <p>Additionally supported by 2D: Australian Post, British Post (4 state code and “infomail”), Data Matrix, Japanese Post, KIX (Netherlands) Post, Planet Code, Postnet, QR Code, EAN/UCC Composite, TCIF Linked Code 39 (TLC39).</p>
Supported Aiming Modes	Class 2 Laser, cross hair with bright center for sunlight visibility; Pick List mode option.
Interface	<p>Cordless: Bluetooth: Class II, v 2.1 with Adaptive Frequency Hopping (AFH). Supported profiles: Serial Port Profile (SPP), Human Interface Device Profile (HID), Service Discovery Application Profile (SDAP). Pairing: by reading terminal BT address as bar code off the display or from a printed label.</p> <p>Corded (to WT4090): Serial.</p>
Field Replaceable Parts	Batteries, corded adaptor, trigger clamp, triggerless clamp, comfort pad, straps and strap buckle.
User Interface	
LED	Two (parallel), multi color, rear left and rear right.
Beeper	Rear center, up to 80 dBA SPL @ 10 cm.
Restore Key	User accessible for emergency boot up and Bluetooth reconnect (after excessive disconnection period).
Scan Triggering	Manual or automatic using Interactive Sensing Technology (IST).
User Environment	
Operating Temperature	-20 °C to 55 °C (-4 °F to 131 °F)
Storage Temperature	-40° to 70° C (-40° to 158° F) excluding battery -40° to 60° C (-40° to 140° F) including battery
Humidity	5% to 85% non condensing
Drop Specification	1.8 m (6 ft.) multiple drops to concrete across operating temperature range.

Table A-4 RS507 Technical Specifications (Continued)

Item	Description
Environmental Sealing	IP54
Electrostatic Discharge (ESD)	±15kV air discharge, ±8kV direct discharge.
Power	
Cordless	Standard battery: Li-Ion 970 mAh, 3.7 V with up to 35,000 scans (continuous) or up to 10 hours with 900 scans per hour on a single charge using fresh batteries. Extended battery: Li-Ion 1940 mAh, 3.7 V with up to 70,000 scans (continuous) or up to 20 hours with 900 scans per hour on a single charge using fresh batteries.
Corded	Corded adaptor to WT4090.
Regulatory	
Electrical Safety	Certified to UL60950-1, CSA C22.2 No. 60950-1, EN60950-1, IEC 60950-1
EMI/RFI	FCC Part 15 Class B, ICES-003 Class B, European Union EMC and R&TTE Directives, Australian AS/NZS 60950.1
Laser Safety	CDRH Class II, IEC 60825-1 Class 2
RoHS	Compliance with RoHS standards.

Accessories

Table A-5 Accessory Specifications

	Single Slot USB Cradle	Four Slot Ethernet Cradle	Four Slot Spare Battery Charger
Operating Temperature	32 °F to 122 °F (0 °C to +50 °C)		32 °F to 104 °F (0 °C to +40 °C)
Storage Temperature	-40 °F to 158 °F (-40 °C to 70 °C)		
Battery Charging Temperature	32 °F to 104 °F (0 °C to +40 °C) ambient temperature		
Humidity	5% to 95% non-condensing		
Size (L x W x H)	6.6 in. x 5.1 in. x 3.9 in. (16.8 cm x 13.0 cm x 9.9 cm)	6.7 in. x 18.9 in. x 4.5 in. (17.0 cm x 48.1 cm x 11.4 cm)	8.5 in. x 5.7 in. x 1.9 in. (21.5 cm x 14.5 cm x 4.9 cm)
Weight	12.1 oz. (344 gm)	45.9 oz. (1300 gm)	15.3 oz. (435 gm)
Power Supply	12 VDC, 3.3 A	12 VDC, 9 A	12 VDC, 3.3 A
Drop	30 inches (76.2 cm) to vinyl covered concrete		
Electrostatic Discharge (ESD)	±15 kV air discharge, ± 8 kV contact discharge		
Typical Power	20 W	60 W	25 W

Wearable Terminal Interface Connector Pin-Outs

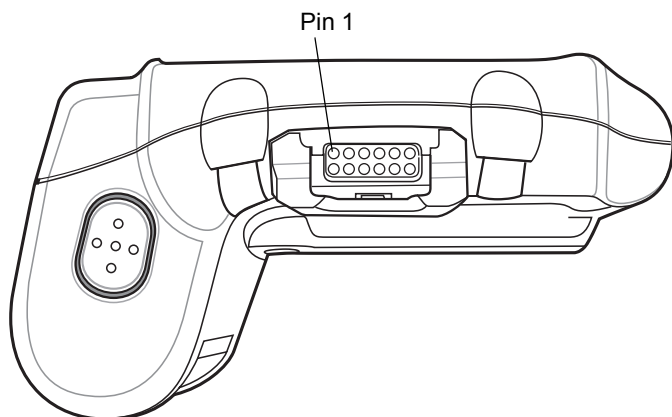


Figure A-1 Pin Locations

Table A-6 Interface Connector Pin-Outs

PIN	Signal Name	Function
1	SCANNER_DETECT_RIGHT	Scanner detect.
2	USBH_N_RIGHT	USB host negative.
3	GND	Digital/system ground.
4	USBH_P_RIGHT	USB host positive.
5	A_GND	Analog ground.
6	HPOUTL_RIGHT_MIC+	Mic+ (default) or headphone out left.
7	U2_RXD	Scanner serial RXD.
8	HPOUTER_RIGHT	Headphone out right.
9	U2_TXD	Scanner serial TXD.
10	SCAN_PWR	Scanner 3.3 VDC power out.
11	U2_CTS	Scanner serial CTS (default if laser scanner plugged in), or Audio Ground sense/MIC- (default if audio connector plugged in).
12	U2_RTS	Scanner serial RTS.

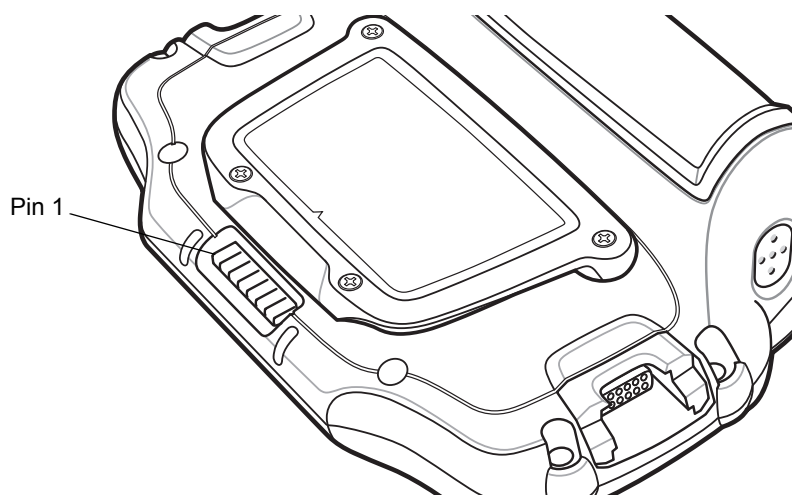


Figure A-2 Cradle Connector Pin Locations

Table A-7 Cradle Connector Pin-Outs

PIN Number	Signal Name	Function
1	Power In	5.4 VDC input power.
2	ACC_OTG_VBUS	5.0 VDC input in client mode, 5.0 VDC output in host mode.
3	ACC_OTG_DP	USB data positive.
4	ACC_OTG_DM	USB data negative.
5	System GND	System ground.
6	ACC_OTG_ID	USB host/client ID pin input. (Low = USB Host, High = USB Client).
7	System Ground	System ground.

Glossary

Numeric

802.11. A group of wireless specifications developed by the Institute of Electrical and Electronics Engineers (IEEE). It specifies an over-the-air interface between a wireless client and a base station or between two wireless clients.

802.11a. Operates in the 5 GHz frequency range (5.125 to 5.85 GHz) with a maximum 54Mbit/sec. signaling rate. The 5 GHz frequency band is not as crowded as the 2.4 GHz frequency because it offers significantly more radio channels than the 802.11b and is used by fewer applications. It has a shorter range than 802.11g and is not compatible with 802.11b.

802.11b. Operates in the 2.4 GHz Industrial, Scientific and Measurement (ISM) band (2.4 to 2.4835 GHz) and provides signaling rates of up to 11Mbit/sec. This is a very commonly used frequency. Microwave ovens, cordless phones, medical and scientific equipment, as well as Bluetooth devices, all work within the 2.4 GHz ISM band.

802.11g. Similar to 802.11b, but this standard supports signaling rates of up to 54Mbit/sec. It also operates in the heavily used 2.4 GHz ISM band but uses a different radio technology to boost overall throughput. Compatible with the 802.11b.

A

Access Point. Provides a bridge between Ethernet wired LANs and the wireless network. Access points are the connectivity point between Ethernet wired networks and devices (laptops, hand-held computers, point-of-sale terminals) equipped with a wireless LAN adapter card.

Ad Hoc Mode. A wireless network framework in which devices communicate directly with one another without using an access point.

API. An interface by means of which one software component communicates with or controls another. Usually used to refer to services provided by one software component to another, usually via software interrupts or function calls

Application Programming Interface. See **API**.

ANSI Terminal. A display terminal that follows commands in the ANSI standard terminal language. For example, it uses escape sequences to control the cursor, clear the screen and set colors. Communications programs support the ANSI terminal mode and often default to this terminal emulation for dial-up connections to online services.

Association. The process of determining the viability of the wireless connection and establishing a wireless network's root and designated access points. A wearable terminal associates with its wireless network as soon as it is powered on or moves into range.

Autodiscrimination. The ability of an interface controller to determine the code type of a scanned bar code. After this determination is made, the information content is decoded.

B

Bar Code. A pattern of variable-width bars and spaces which represents numeric or alphanumeric data in machine-readable form. The general format of a bar code symbol consists of a leading margin, start character, data or message character, check character (if any), stop character, and trailing margin. Within this framework, each recognizable symbology uses its own unique format. See **Symbology**.

Bit. Binary digit. One bit is the basic unit of binary information. Generally, eight consecutive bits compose one byte of data. The pattern of 0 and 1 values within the byte determines its meaning.

Bits per Second (bps). Bits transmitted or received.

Bluetooth. A low-cost, short-range radio link between two devices. Bluetooth can replace cables and can be used to create ad hoc networks and provide a standard way to connect devices.

Bit. Binary digit. One bit is the basic unit of binary information. Generally, eight consecutive bits compose one byte of data. The pattern of 0 and 1 values within the byte determines its meaning.

bps. See **Bits Per Second**.

Byte. On an addressable boundary, eight adjacent binary digits (0 and 1) combined in a pattern to represent a specific character or numeric value. Bits are numbered from the right, 0 through 7, with bit 0 the low-order bit. One byte in memory is used to store one ASCII character.

boot or boot-up. The process a computer goes through when it starts. During boot-up, the computer can run self-diagnostic tests and configure hardware and software.

C

CAM. (Continuously Aware Mode) Mode in which the adapter is instructed to continually check for network activity.

CDRH. (Center for Devices and Radiological Health) A federal agency responsible for regulating laser product safety. This agency specifies various laser operation classes based on power output during operation.

CDRH Class 1. This is the lowest power CDRH laser classification. This class is considered intrinsically safe, even if all laser output were directed into the eye's pupil. There are no special operating procedures for this class.

CDRH Class 2. No additional software mechanisms are needed to conform to this limit. Laser operation in this class poses no danger for unintentional direct human exposure.

CHAP. (Challenge Handshake Authentication Protocol) A type of authentication in which the authentication agent (typically a network server) sends the client program a random value that is used only once and an ID value. Both the sender and peer share a predefined secret. The peer concatenates the random value (or nonce), the ID and the secret and calculates a one-way hash using MD5. The hash value is sent to the authenticator, which in turn builds that same string on its side, calculates the MD5 sum itself and compares the result with the value received from the peer. If the values match, the peer is authenticated.

Character. A pattern of bars and spaces which either directly represents data or indicates a control function, such as a number, letter, punctuation mark, or communications control contained in a message.

Character Set. Those characters available for encoding in a particular bar code symbology.

Check Digit. A digit used to verify a correct symbol decode. The scanner inserts the decoded data into an arithmetic formula and checks that the resulting number matches the encoded check digit. Check digits are required for UPC but are optional for other symbologies. Using check digits decreases the chance of substitution errors when a symbol is decoded.

Cold Boot. A cold boot restarts the wearable terminal and erases all user stored records and entries.

COM port. Communication port; ports are identified by number, e.g., COM1, COM2.

Continuous Code. A bar code or symbol in which all spaces within the symbol are parts of characters. There are no intercharacter gaps in a continuous code. The absence of gaps allows for greater information density.

Cradle. A cradle is used for charging the terminal battery and for communicating with a host computer, and provides a storage place for the terminal when not in use.

D

Data Communications Equipment (DCE). A device (such as a modem) which is designed to attach directly to a DTE (Data Terminal Equipment) device.

DCE. See **Data Communications Equipment**.

DCP. See **Device Configuration Package**.

Decode. To recognize a bar code symbology (e.g., UPC/EAN) and then analyze the content of the specific bar code scanned.

Decode Algorithm. A decoding scheme that converts pulse widths into data representation of the letters or numbers encoded within a bar code symbol.

Decryption. Decryption is the decoding and unscrambling of received encrypted data. Also see, **Encryption** and **Key**.

Depth of Field. The range between minimum and maximum distances at which a scanner can read a symbol with a certain minimum element width.

Device Configuration Package. The Device Configuration Package provides flash partitions, Terminal Configuration Manager (TCM) and the associated TCM scripts. With this package hex images that represent flash partitions can be created and downloaded to the wearable terminal.

DTE. See **Data Terminal Equipment**.

E

EAN. (European Article Number) This European/International version of the UPC provides its own coding format and symbology standards. Element dimensions are specified metrically. EAN is used primarily in retail.

EAP. (Extensible Authentication Protocol) A general authentication protocol used to control network access. Many specific authentication methods work within this framework.

EAP-PEAP. (Extensible Authentication Protocol-Protected Extensible Authentication Protocol) A mutual authentication method that uses a combination of digital certificates and another system, such as passwords.

EAP-TLS. (Extensible Authentication Protocol-Transport Layer Security) A mutual authentication method that uses digital certificates.

Encoded Area. Total linear dimension occupied by all characters of a code pattern, including start/stop characters and data.

Encryption. Encoding data to prevent it from being read by unauthorized people.

ENQ (RS-232). ENQ software handshaking is also supported for the data sent to the host.

EMDK. Enterprise Mobility Developer's Kit.

Ethernet . An IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium.

ESD. Electro-Static Discharge

F

Flash Disk. An additional megabyte of non-volatile memory for storing application and configuration files.

Flash Memory. Flash memory is nonvolatile, semi-permanent storage that can be electronically erased in the circuit and reprogrammed.

File Transfer Protocol (FTP). A TCP/IP application protocol governing file transfer via network or telephone lines. See **TCP/IP**.

H

Hard Reset. See **Cold Boot**.

Hz. Hertz; A unit of frequency equal to one cycle per second.

Host Computer. A computer that serves other terminals in a network, providing such services as computation, database access, supervisory programs and network control.

I

IEC. International Electrotechnical Commission. This international agency regulates laser safety by specifying various laser operation classes based on power output during operation.

IEC (825) Class 1. This is the lowest power IEC laser classification. Conformity is ensured through a software restriction of 120 seconds of laser operation within any 1000 second window and an automatic laser shutdown if the scanner's oscillating mirror fails.

IEEE Address. See **MAC Address**.

Internet Protocol Address. See **IP**.

I/O Ports. interface The connection between two devices, defined by common physical characteristics, signal characteristics, and signal meanings. Types of interfaces include RS-232 and PCMCIA.

Input/Output Ports. I/O ports are primarily dedicated to passing information into or out of the terminal's memory. Series 9000 wearable terminals include Serial and USB ports.

IP. (Internet Protocol) The IP part of the TCP/IP communications protocol. IP implements the network layer (layer 3) of the protocol, which contains a network address and is used to route a message to a different network or subnetwork. IP accepts "packets" from the layer 4 transport protocol (TCP or UDP), adds its own header to it and delivers a "datagram" to the layer 2 data link protocol. It may also break the packet into fragments to support the maximum transmission unit (MTU) of the network.

IP Address. (Internet Protocol address) The address of a computer attached to an IP network. Every client and server station must have a unique IP address. A 32-bit address used by a computer on a IP network. Client workstations have either a permanent address or one that is dynamically assigned to them each session. IP addresses are written as four sets of numbers separated by periods; for example, 204.171.64.2.

IPX/SPX. Internet Package Exchange/Sequential Packet Exchange. A communications protocol for Novell. IPX is Novell's Layer 3 protocol, similar to XNS and IP, and used in NetWare networks. SPX is Novell's version of the Xerox SPP protocol.

IS-95. Interim Standard 95. The EIA/TIA standard that governs the operation of CDMA cellular service. Versions include IS-95A and IS-95B. See CDMA.

K

Key. A key is the specific code used by the algorithm to encrypt or decrypt the data. Also see, **Encryption** and **Decrypting**.

L

laser scanner. A type of bar code reader that uses a beam of laser light.

LASER. (Light Amplification by Stimulated Emission of Radiation) The laser is an intense light source. Light from a laser is all the same frequency, unlike the output of an incandescent bulb. Laser light is typically coherent and has a high energy density.

LCD. See **Liquid Crystal Display**.

LEAP. (Lightweight Extensible Authentication Protocol) A mutual authentication method that uses a username and password system.

LED Indicator. A semiconductor diode (LED - Light Emitting Diode) used as an indicator, often in digital displays. The semiconductor uses applied voltage to produce light of a certain frequency determined by the semiconductor's particular chemical composition.

Liquid Crystal Display (LCD). A display that uses liquid crystal sealed between two glass plates. The crystals are excited by precise electrical charges, causing them to reflect light outside according to their bias. They use little electricity and react relatively quickly. They require external light to reflect their information to the user.

M

MC. Mobile computer.

MDN. (Mobile Directory Number) The directory listing telephone number that is dialed (generally using POTS) to reach a mobile unit. The MDN is usually associated with a MIN in a cellular telephone -- in the US and Canada, the MDN and MIN are the same value for voice cellular users. International roaming considerations often result in the MDN being different from the MIN.

MIL. 1 mil = 1 thousandth of an inch.

MIN. (Mobile Identification Number) The unique account number associated with a cellular device. It is broadcast by the cellular device when accessing the cellular system.

MS CHAP. (Microsoft Challenge Handshake Authentication Protocol) is the Microsoft version of CHAP and is an extension to RFC 1994. Like the standard version of CHAP, MS-CHAP is used for PPP authentication; in this case, authentication occurs between a PC using Microsoft Windows NT or Microsoft Windows 95 and a Cisco router or access server acting as a network access server (NAS).

N

Nominal. The exact (or ideal) intended value for a specified parameter. Tolerances are specified as positive and negative deviations from this value.

Nominal Size. Standard size for a bar code symbol. Most UPC/EAN codes are used over a range of magnifications (e.g., from 0.80 to 2.00 of nominal).

NVM. Non-Volatile Memory.

O

ODI. See **Open Data-Link Interface**.

Open Data-Link Interface (ODI). Novell's driver specification for an interface between network hardware and higher-level protocols. It supports multiple protocols on a single NIC (Network Interface Controller). It is capable of understanding and translating any network information or request sent by any other ODI-compatible protocol into something a NetWare client can understand and process.

Open System Authentication. Open System authentication is a null authentication algorithm.

P

PAN . Personal area network. Using Bluetooth wireless technology, PANs enable devices to communicate wirelessly. Generally, a wireless PAN consists of a dynamic group of less than 255 devices that communicate within about a 33-foot range. Only devices within this limited area typically participate in the network.

Parameter. A variable that can have different values assigned to it.

PING. (Packet Internet Groper) An Internet utility used to determine whether a particular IP address is online. It is used to test and debug a network by sending out a packet and waiting for a response.

Programming Mode. The state in which a scanner is configured for parameter values. See **Scanning Mode**.

Q

Quiet Zone. A clear space, containing no dark marks, which precedes the start character of a bar code symbol and follows the stop character.

R

RAM. Random Access Memory. Data in RAM can be accessed in random order, and quickly written and read.

RF. Radio Frequency.

ROM. Read-Only Memory. Data stored in ROM cannot be changed or removed.

Router. A device that connects networks and supports the required protocols for packet filtering. Routers are typically used to extend the range of cabling and to organize the topology of a network into subnets. See **Subnet**.

RS-232. An Electronic Industries Association (EIA) standard that defines the connector, connector pins, and signals used to transfer data serially from one device to another.

S

Scanner. An electronic device used to scan bar code symbols and produce a digitized pattern that corresponds to the bars and spaces of the symbol. Its three main components are:

1. Light source (laser or photoelectric cell) - illuminates a bar code.
2. Photodetector - registers the difference in reflected light (more light reflected from spaces).
3. Signal conditioning circuit - transforms optical detector output into a digitized bar pattern.

Scanning Mode. The scanner is energized, programmed and ready to read a bar code.

Scanning Sequence. A method of programming or configuring parameters for a bar code reading system by scanning bar code menus.

SDK. Software Development Kit

Secure Sockets Layer (SSL). SSL is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL is included as part of both the Microsoft and Netscape browsers and most Web server products. Developed by Netscape, SSL also gained the support of Microsoft and other Internet client/server developers as well and became the de facto standard until evolving into Transport Layer Security. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

Shared Key. Shared Key authentication is an algorithm where both the AP and the MU share an authentication key.

Soft Reset. See **Warm Boot**.

Specular Reflection. The mirror-like direct reflection of light from a surface, which can cause difficulty decoding a bar code.

Subnet. A subset of nodes on a network that are serviced by the same router. See **Router**.

Subnet Mask. A 32-bit number used to separate the network and host sections of an IP address. A custom subnet mask subdivides an IP network into smaller subsections. The mask is a binary pattern that is matched up with the IP address to turn part of the host ID address field into a field for subnets. Default is often 255.255.255.0.

Substrate. A foundation material on which a substance or image is placed.

Symbol. A scannable unit that encodes data within the conventions of a certain symbology, usually including start/stop characters, quiet zones, data characters and check characters.

Symbology. The structural rules and conventions for representing data within a particular bar code type (e.g. UPC/EAN, Code 39, PDF417, etc.).

T

TCP/IP. (Transmission Control Protocol/Internet Protocol) A communications protocol used to internetwork dissimilar systems. This standard is the protocol of the Internet and has become the global standard for communications. TCP provides transport functions, which ensures that the total amount of bytes sent is received correctly at the other end. UDP is an alternate transport that does not guarantee delivery. It is widely used for real-time voice and video transmissions where erroneous packets are not retransmitted. IP provides the routing mechanism. TCP/IP is a routable protocol, which means that all messages contain not only the address of the destination station, but the address of a destination network. This allows TCP/IP messages to be sent to multiple networks within an organization or around the world, hence its use in the worldwide Internet. Every client and server in a TCP/IP network requires an IP address, which is either permanently assigned or dynamically assigned at startup.

Telnet. A terminal emulation protocol commonly used on the Internet and TCP/IP-based networks. It allows a user at a terminal or computer to log onto a remote device and run a program.

Terminal Emulation. A “terminal emulation” emulates a character-based mainframe session on a remote non-mainframe terminal, including all display features, commands and function keys. The WT4090 Series supports Terminal Emulations in 3270, 5250 and VT220.

TFTP. (Trivial File Transfer Protocol) A version of the TCP/IP FTP (File Transfer Protocol) protocol that has no directory or password capability. It is the protocol used for upgrading firmware, downloading software and remote booting of diskless devices.

TKIP. (Temporal Key Integrity Protocol) A wireless encryption protocol that periodically changes the encryption key, making it harder to decode.

Tolerance. Allowable deviation from the nominal bar or space width.

Transmission Control Protocol/Internet Protocol. See **TCP/IP.**

TLS. (Transport Layer Security) TLS is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

Trivial File Transfer Protocol. See **TFTP.**

TSR. See **Terminate and Stay Resident.**

U

UDP. (User Datagram Protocol) A protocol within the IP protocol suite that is used in place of TCP when a reliable delivery is not required. For example, UDP is used for real-time audio and video traffic where lost packets are simply ignored, because there is no time to retransmit. If UDP is used and a reliable delivery is required, packet sequence checking and error notification must be written into the applications.

U

Visible Laser Diode (VLD). A solid state device which produces visible laser light.

W

Warm Boot. A warm boot restarts the wearable terminal by closing all running programs. All data that is not saved to flash memory is lost.

WAP. (Wireless Application Protocol) A set of specifications, developed by the WAP Forum, that lets developers using Wireless Markup Language build networked applications designed for handheld wireless devices. WAP was designed to work within the constraints of these devices: a limited memory and CPU size, small, monochrome screens, low bandwidth and erratic connections.

Wearable Terminal. In this text, wearable terminal refers to the WT4070/90 wireless portable computer. It can be set up to run as a stand-alone device, or it can be set up to communicate with a network, using wireless radio technology.

WEP. Wired-Equivalent Privacy protocol was specified in the IEEE 802.11 standard to provide a WLAN with a minimal level of security and privacy comparable to a typical wired LAN, using data encryption.

WPA. Wi-Fi Protected Access is a data encryption specification for 802.11 wireless networks that replaces the weaker WEP. It improves on WEP by using dynamic keys, Extensible Authentication Protocol to secure network access, and an encryption method called Temporal Key Integrity Protocol (TKIP) to secure data transmissions.

WPA2. Wi-Fi Protected Access 2 is an enhanced version of WPA. It uses Advanced Encryption Standard instead of TKIP.

WLAN. Wireless local-area networks use radio waves instead of a cable to connect a user device, such as a wearable terminal, to a LAN. They provide Ethernet connections over the air and operate under the 802.11 family of specifications developed by the IEEE.

Index

Numerics

128-Bit WEP	5-15
40-Bit WEP	5-15
802.11 ESSID	5-5
802.11d	5-34

A

accessories	
four slot Ethernet cradle	2-6
four slot spare battery charger	2-1
serial cradle	2-1
single slot serial/USB cradle	2-2
LED indicators	2-4, 2-12
spare battery charger	2-11
power connection	2-11
ActiveSync	3-1
downloading files	7-3
installing	3-1
setting up a connection	3-2
Adaptive Frequency Hopping	6-1
ad-hoc	5-6
ad-hoc mode	5-5, 5-7
ad-hoc networks	5-34
Advanced Encryption Standard	5-16
AES	5-16
AFH	6-1
AP networks	5-34
authentication	5-7
EAP-TLS	5-8
LEAP	5-8
none	5-8
PEAP	5-8
tunneled	5-8
automatic time setting	5-36

B

backup battery	
charging	1-5
band selection	
2.4 GHz	5-35
5 GHz	5-35
battery	
backup charging	1-5
charging	1-5
temperature range	A-9
check status	1-7
installing	1-4
removing	1-6
battery charging temperature	A-2
battery management	1-8
bluetooth	
adaptive frequency hopping	6-1
ad-hoc mode	5-6
bonding	6-17
deleting bonded device	6-20
discovering devices	6-7
turning off	6-3
turning on	6-3
Bluetooth security	6-2
bonding, bluetooth	6-17
boot	
cold	1-7, 1-8, 6-4
warm	1-8, 6-4
bullets	xvi

C

CAM	5-21
changing profile password	5-36
changing the power settings	1-9
charging	

- spare batteries 1-6
- temperature range A-9
- charging batteries 1-5
- charging spare batteries 1-6
- cleaning 10-1
- cold boot 1-7, 1-8, 6-4, 7-21
- configuration xiv
- configurations xiv
- conventions
 - notational xvi
- country code 5-6
- country setting 5-34
- CPU A-1
- cradles
 - Ethernet drivers 2-8
 - four slot Ethernet 2-6
 - charging 2-9
 - serial cradle 2-1
 - single slot 2-2
 - LED indicators 2-4, 2-12
 - spare battery charger 2-11
 - power connection 2-11
- creating a new profile 5-24
- creating splash screen 7-19

D

- data capture xiv
- DCP 7-1
- DCP for WT4090c50 xvii, 7-5, 7-9, 7-19, 7-21
- default gateway 5-18
- deleting a profile 5-24
- deleting bluetooth bond 6-20
- Device Configuration Package 7-1
- Device Configuration Package for WT4090c50 xvii, 7-5, 7-9, 7-19, 7-21
- DHCP 5-18
- dimensions A-1, A-4, A-5, A-7
- display xiv, A-1
- display backlight
 - saving power 1-9
- DNS 5-18, 5-20
- downloading files 7-3
- drop specification A-2, A-5, A-6, A-8

E

- EAP-TLS 5-8
- edit a profile 5-4
- electrical safety A-4, A-5, A-6, A-9
- EMDK for eVC4 xvii
- encryption 5-15
 - open system 5-16, 5-18
 - TKIP (WPA) 5-16

- Enterprise Mobility Developer Kit for eVC4 xvii
- error messages 7-16, 7-17
- exporting a profile 5-24, 5-37

F

- Fast Power Save 5-21
- file explorer 7-6
- finding access points 5-3
- finding WLAN networks 5-3
- flash file system 7-20
 - downloading partitions 7-22
 - non-FFS partitions 7-22
 - IPL 7-22
 - splash screen 7-22
 - partitions 7-20
 - copyfile 7-21
 - regmerge 7-21
- flash storage 7-20
- four slot Ethernet cradle 2-6, 2-15
 - charging 2-9
 - drivers 2-8
- four slot spare battery charger 2-1, 2-17
- Fusion version 5-29

G

- gateway 5-20
- getting started 1-4

H

- hard reset 1-7, 1-8, 6-4
- humidity A-2, A-5, A-6, A-8

I

- information, service xvii
- infrastructure 5-6
- infrastructure mode 5-5
- Initial Program Loader 7-22
- installing development tools 7-2
- installing main battery 1-4
- IP address 5-18, 5-19
- IP config
 - DNS 5-20
 - gateway 5-20
 - IP address 5-19
 - subnet mask 5-19
 - WINS 5-20
- IP management 5-36
- IPL 7-22
 - error messages 7-17
 - error screen 7-17

K

- keyboard A-1
- keypad backlight
 - saving power 1-9
- keypadsxiv
- known APs
 - APs 5-32

L

- laser safety A-5, A-6, A-9
- LEAP 5-8
- lithium-ion battery 1-1
- log
 - wireless log 5-29

M

- main battery
 - charging 1-4, 1-5
 - temperature range A-9
 - installing 1-4
- maintenance 10-1
- managing profiles 5-22
- MAX Power Save 5-21
- memoryxiv, A-2
- mode
 - 802.11 ESSID 5-5
 - ad-hoc 5-6
 - country 5-6
 - infrastructure 5-6
 - operating 5-6
 - profile name 5-5

O

- open system5-16, 5-18
- operating environment, wearable terminal A-1
- operating mode 5-6
- operating mode filtering 5-33
- operating systemxiv, A-2
- operating temperature A-2, A-5, A-6, A-8
- ordering profiles 5-24

P

- packet tracing 5-31
- partitions
 - downloading 7-22
 - FFS 7-20
 - non-FFS 7-22
 - IPL 7-22
 - splash screen 7-22

- parts of the wearable terminal 1-1, 1-2, 1-3
- PassKey 5-17
- password 5-14
- PEAP 5-8
- ping 5-31
- pin-outs
 - wearable terminal A-10
- power settings 1-9
- power supply 2-14
- profile
 - create new 5-24
 - delete 5-24
 - edit 5-4
- profile ID 5-4
- profile name 5-5
- profile persistence 5-38
- profile roaming 5-36
- programs
 - flash file system 7-20

R

- radiosxiv
- registry settings 5-38
- regulatory options 5-34
- removing main battery 1-6
- reset
 - hard 1-7, 1-8, 6-4
 - soft 1-8, 6-4
- resetting 1-8
- resume 6-4

S

- scripts
 - creating 7-8
 - saving 7-9
- serial cradle 2-1
- server certificate 5-11
- service information xvii
- setting up a partnership
 - partnership 3-3
- signal strength 5-3, 5-25, 5-26
- signal strength icon 5-2
- single slot serial/USB cradle 2-2
 - LED indicators 2-4, 2-12
- SMDK for C 7-1
- soft reset 1-8, 6-4
- spare batteries
 - charging 1-6
- spare battery
 - charging 1-6
- spare battery charger
 - power connection 2-11

splash screen 7-22
 creating 7-19
 starting the wearable terminal 1-4, 1-7
 static 5-18
 storage temperature A-2, A-5, A-6, A-8
 subnet mask 5-19
 suspend 1-6, 6-4
 Symbol Mobility Developer Kit for C 7-1

wireless status 5-25
 WLAN 802.11a/b/g xiv
 WLAN radio
 turn on 5-3
 turning off 5-3
 WPAN Bluetooth xiv

T

TCM
 building hex image 7-5, 7-9, 7-10
 creating script 7-8
 defining properties 7-7
 error messages 7-16
 hex image download 7-11
 saving script 7-9
 starting 7-6
 technical specifications, wearable terminal A-1
 temperature
 battery charging A-9
 TKIP 5-16
 TKIP (WPA) 5-16
 transmit power
 automatic 5-20
 power plus 5-20
 troubleshooting 10-6
 four slot spare battery charger 10-10
 turn the radios off
 saving power 1-10

U

unpacking 1-1
 user certificate 5-10
 user name 5-14

W

wall mounting bracket 2-13
 mounting multiple brackets 2-19
 wiring 2-17
 warm boot 1-8, 6-4
 wearable terminal
 cold boot 7-21
 starting 1-7
 weight A-1, A-4, A-5, A-7
 WINS 5-18, 5-20
 wireless diagnostics
 diagnostics 5-30
 Wireless Local Area Networks 5-1
 wireless options 5-33
 wireless registry settings 5-38



Zebra Technologies Corporation
Lincolnshire, IL U.S.A.
<http://www.zebra.com>

Zebra and the stylized Zebra head are trademarks of ZIH Corp., registered in many jurisdictions worldwide. All other trademarks are the property of their respective owners.

©2015 ZIH Corp and/or its affiliates. All rights reserved.