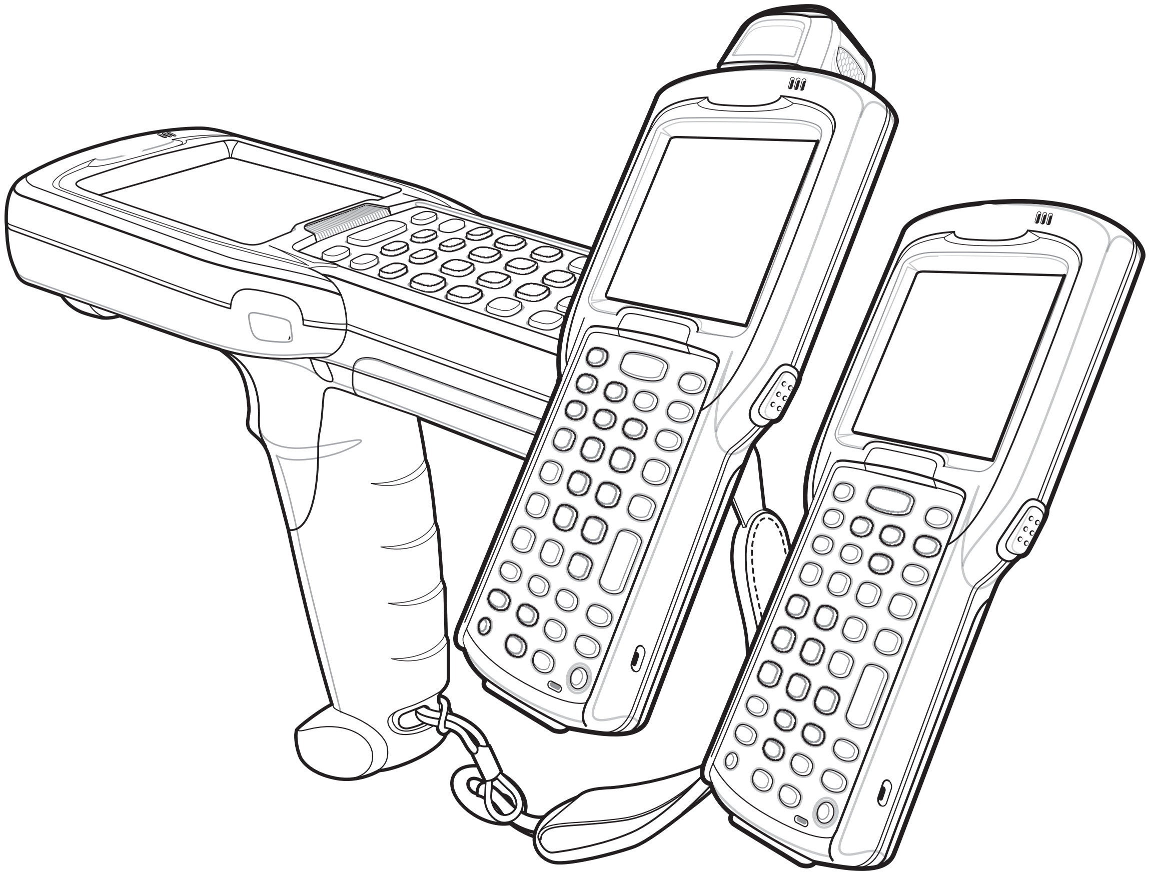
MC3000

Integrator Guide



MC3000 Mobile Computer

Integrator Guide

72E-68900-06

Revision A

April 2015

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	Dec. 2004	Initial Release
-01 Rev B	June 2005	Added Four Slot Ethernet cradle.
		Appendix A, added Accessory Specifications.
-02 Rev A	November 2005	Chapter 7, removed WZC, replaced with wireless application description. Global changes: Changed Windows CE.NET 4.2 to Windows CE.NET 5.0 Removed WZC references, replaced with wireless application references. Added 802.11a. Page 2-9 and 2-10 added Four Slot Ethernet cradle.
-02 Rev B	June 2006	Add Direct Part Marking information, MC3090S 128 MB RAM/64 MB Flash configuration and update SMDK information.
-03 Rev A	March 2007	Add 20-key mechanical keypad and Fusion 2.5 information.
-04 Rev A	August 2007	Motorola re-branding. Operating system update: OEM Version 05.26.0000.
-05 Rev A	October 2008	Add Windows Mobile 6.1 configurations.
-06 Rev A	April 2015	Zebra re-branding.

Table of Contents

About This Guide

Chapter 1: Getting Started

Chapter 2: Accessories

Chapter 3: ActiveSync

Chapter 4: Application Deployment for Windows CE 5.0

Chapter 5: Application Deployment for Windows Mobile 6.1

Chapter 6: Wireless Applications

Chapter 7: Staging and Provisioning

Chapter 8: Maintenance & Troubleshooting

Appendix A: Technical Specifications

Appendix B: Internet Explorer Kiosk Mode

Glossary

Index

About This Guide

Introduction

This guide provides information about setting up and configuring MC3000 mobile computers and accessories.

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

Documentation Set

The documentation set for the MC3000 is divided into guides that provide information for specific user needs.

- Microsoft Application Guide for Mobile and WinCE 5.0 User Guide - describes how to use Microsoft developed applications.
- Microsoft Application Guide for Windows Mobile 6 User Guide - describes how to use Microsoft developed applications.
- Application Guide for Zebra Devices - describes how to use Zebra developed applications.
- MC3000 User Guide - describes how to use the MC3000 mobile computer.
- MC3000 Integrator Guide - describes how to set up the MC3000 mobile computer 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
MC3000R	None	Color or monochrome	32 MB RAM/ 64 MB Flash or 64 MB RAM/ 64 MB Flash	1D laser scanner in rotating turret	Windows CE 5.0 Core or Professional	28, 38 or 48 key
MC3090G	WLAN: 802.11a/b/g WPAN: Bluetooth	Color or monochrome	32 MB RAM/ 64 MB Flash or 64 MB RAM/ 64 MB Flash	1D laser scanner or 2D imager	Windows CE 5.0 Core or Professional	28, 38 or 48 key
MC3090S	WLAN: 802.11a/b/g WPAN: Bluetooth	Color	64 MB RAM/ 64 MB Flash or 128 MB RAM/ 64 MB Flash or 128 MB RAM/64 MB Flash + 1GB Flash storage	1D laser scanner, 2D imager or DPM Imager	Windows CE 5.0 Professional or Windows Mobile 6.1 Classic	28, 38, 48 key or 20 key Mechanical
MC3090R	WLAN: 802.11a/b/g WPAN: Bluetooth	Color or monochrome	32 MB RAM/ 64 MB Flash or 128 MB RAM/64 MB Flash + 1GB Flash storage	1D laser scanner in rotating turret	Windows CE 5.0 Core or Professional or Windows Mobile 6.1 Classic	28, 38, 48 key or 20 key Mechanical

Software Versions

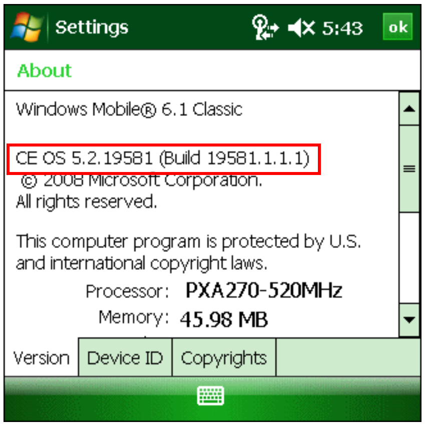
This guide covers various software configurations and references are made to operating system or software versions for:

- Adaptation Kit Update (AKU) version
- OEM version
- BTExplorer version
- Fusion version.

AKU Version for Windows Mobile 6.1 Devices

To determine the Adaptation Kit Update (AKU) version on a Windows Mobile 6.1 device:

Tap **Start** > **Settings** > **System** tab > **About** icon > **Version** tab.



Windows Mobile® 6.1 Classic

CE OS 5.2.19581 (Build 19581.1.1.1)
© 2008 Microsoft Corporation.
All rights reserved.

This computer program is protected by U.S. and international copyright laws.

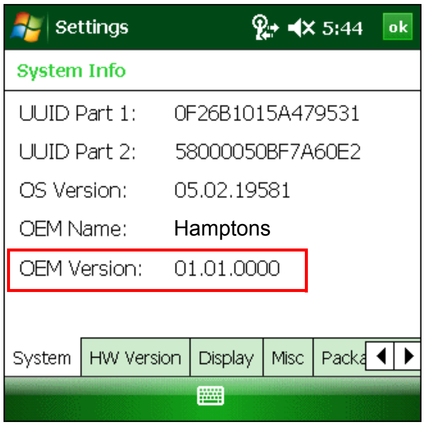
Processor: PXA270-520MHz
Memory: 45.98 MB

The second line lists the operating system version and the build number. The last part of the build number represents the AKU number. For example, *Build 119581.1.1.1* indicates that the device is running AKU version *1.1.1*.

OEM Version on Windows Mobile 6.1 Devices

To determine the OEM software version on a Windows Mobile 6.1 device:

Tap **Start** > **Settings** > **System** tab > **System Information** icon > **System** tab.

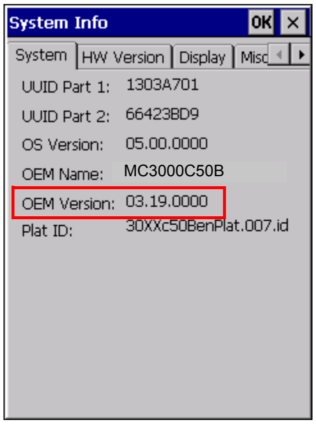


UUID Part 1: 0F26B1015A479531
UUID Part 2: 58000050BF7A60E2
OS Version: 05.02.19581
OEM Name: Hamptons
OEM Version: 01.01.0000

OEM Software on Windows CE 5.0 Devices

To determine the OEM software version on a Windows CE 5.0 device:

Tap **Start** > **Settings** > **Control Panel** > **System Information** icon > **System** tab.

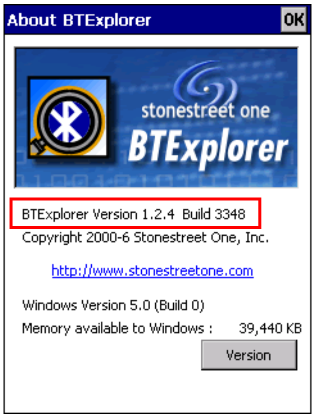


UUID Part 1: 1303A701
UUID Part 2: 66423BD9
OS Version: 05.00.0000
OEM Name: MC3000C50B
OEM Version: 03.19.0000
Plat ID: 30XXc50BenPlat.007.id

BTExplorer Software

To determine the BTExplorer software version on a Windows Mobile 6.1 or Windows CE 5.0 device:

Tap **BTExplorer** icon > **Show BTExplorer**> **File** > **About**.



BTExplorer Version 1.2.4 Build 3348
Copyright 2000-6 Stonestreet One, Inc.

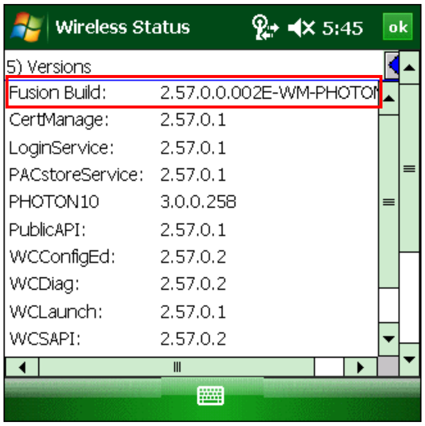
http://www.stonestreetone.com

Windows Version 5.0 (Build 0)
Memory available to Windows : 39,440 KB

Fusion Software

To determine the Fusion software version on a Windows Mobile 6.1 or Windows CE 5.0 device:

Tap **Wireless Strength** icon > **Wireless Status** > **Versions**.



5) Versions

Fusion Build:	2.57.0.0.002E-WM-PHOTON
CertManage:	2.57.0.1
LoginService:	2.57.0.1
PACstoreService:	2.57.0.1
PHOTON10	3.0.0.258
PublicAPI:	2.57.0.1
WCConfigEd:	2.57.0.2
WCDiag:	2.57.0.2
WCLaunch:	2.57.0.1
WCSAPI:	2.57.0.2

Chapter Descriptions

Topics covered in this guide are as follows:

- *Chapter 1, Getting Started*, describes the mobile computer’s physical characteristics, how to install and charge the batteries, remove and replace the Strap/Door Assembly and how to start the mobile computer for the first time.
- *Chapter 2, Accessories*, describes the accessories available including cradles, cables and spare battery chargers. Accessory set up and use is also provided.
- *Chapter 3, ActiveSync*, provides instructions on installing ActiveSync, setting up a partnership and synchronizing information between the mobile computer and a host computer.
- *Chapter 4, Application Deployment for Windows CE 5.0*, provides instructions for provisioning and deploying applications on the MC3000 with WinCE 5.0.
- *Chapter 5, Application Deployment for Windows Mobile 6.1*, provides instructions for provisioning and deploying applications on the MC3000 with Windows Mobile 6.1.
- *Chapter 6, Wireless Applications*, describes how to configure the wireless connection and how the wireless LANs allow the mobile computers to communicate wirelessly with a host device.
- *Chapter 7, Staging and Provisioning*, explains how to facilitate software downloads to a mobile device.
- *Chapter 8, Maintenance & Troubleshooting*, includes instructions on cleaning and storing the mobile computer, and provides troubleshooting solutions for potential problems during mobile computer operation.
- *Appendix A, Technical Specifications*, includes a table listing the technical specifications for the mobile computer.
- *Appendix B, Internet Explorer Kiosk Mode*, provides instructions for configuring Internet Explorer’s Kiosk mode.

Notational Conventions

The following conventions are used in this document:

- The term “mobile computer” refers to the Zebra MC3000.
- *Italics* are used to highlight the following:
  - Chapters and sections in this and related documents
  - Dialog box, window and screen names
  - Drop-down list and list box names
  - Check box and radio button names
  - Icons on a screen.
- **Bold** text is used to highlight the following:
  - 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 MC3000 mobile computers.

- *MC3000 Series Quick Start Guide* p/n 72-68902-xx
- *MC3090G Quick Start Guide*, p/n 72-71347-xx
- *MC3000 Licensing, Patent and Regulatory Information*, p/n 72-68903-xx
- *MC3000 Regulatory Guide for Windows Mobile 6, p/n 72-* 72-114046-xx
- *MC3000 User Guide*, p/n 72E-68899-xx
- *Application Guide for Zebra Devices*, p/n 72-68901-xx
- *Microsoft® Applications for Mobile and WinCE 5.0 User Guide*, p/n 72E-78456-xx
- *Microsoft® Applications for Mobile 6 User Guide*, p/n 72E-108299-xx
- *Enterprise Mobility Developer Kit (EMDK) Help File*, p/n 72E-38880-03
- *Windows CE Platform SDK for MC3000c50,* available at: http://www.zebra.com/support
- *Enterprise Mobility Developer Kit for C (SMDK for C),* available at: http://www.zebra.com/support
- Device Configuration Package for MC3000 (DCP for MC3000), available at: http://www.zebra.com/support
- 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 email, 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 describes the mobile computer's physical characteristics, how to install and charge the batteries, how to remove and replace the Strap/Door Assembly and how to start the mobile computer for the first time.

Unpacking the Mobile Computer

Carefully remove all protective material from around the mobile computer and save the shipping container for later storage and shipping. Verify that the equipment listed below is included:

- MC3000 mobile computer
- Strap/Door Assembly, attached to the mobile computer
- Stylus
- Regulatory Guide
- Quick Start Guide (poster).

Depending on the configuration ordered, the mobile computer shipping container or additional shipping container may include:

- Standard Battery (lithium-polymer)
- Extended Life Battery (lithium-ion)
- Cable(s)
- Power Supply
- Cradles.

Inspect the equipment for damage. If any equipment is missing or damaged, contact Zebra Support immediately. See page xvi for contact information.

Accessories

Table 1-1 lists the MC3000 accessories.

Table 1-1 MC3000 Accessories

Accessory	Description
Single Slot Serial/USB Cradle	Charges the mobile computer main battery and a spare battery, and synchronizes the mobile computer with a host computer through either a serial or USB connection.
Four Slot Charge Only Cradle	Charges up to four mobile computers.
Four Slot Ethernet Cradle	Charges up to four mobile computers and provides Ethernet communications.
Four Slot Spare Battery Charger	Charges up to four mobile computer spare batteries.
Power Supply	Country specific and accessory specific, power supply.
USB Client Charge Cable	Provides USB client communication capabilities and charges the mobile computer.
Serial (RS232) Charge Cable	Provides RS232 communication capabilities and charges the mobile computer.
O’Neil Printer Cable	Provides printer specific communication capabilities (provided by O’Neil).
Zebra Printer Cable	Provides printer specific communication capabilities (provided by Zebra).
Monarch Printer Cable	Provides printer specific communication capabilities (provided by Monarch).
Single Slot Cradle RS232 Cable	Provides serial host communication capabilities and charges the mobile computer.
Single Slot Cradle USB Cable	Provides USB communication capabilities and charges the mobile computer.
MC3000 Universal Battery Charger Adapter (UBC)	Adapts the UBC for use with MC3000 batteries.
Stylus	Performs pen and mouse functions.
Plastic Holster	Provides a clip on holder for the mobile computer.
Fabric Holster	Provides a soft, clip on holder and a shoulder strap for the mobile computer.
Symbol Mobility Developer Kit for C	A development tool used to create native C and C++ applications for all Zebra mobile computers running the Microsoft Windows CE operating system. Available at: http://www.zebra.com/support.
Device Configuration Package (DCP) for MC3000	A development tool used to create and download hex images that represent flash partitions to the mobile computer. Available at: http://www.zebra.com/support.

Parts

There are three versions of the MC3000 mobile computers, the MC3000 1D/2D Imager (MC3000S or MC3090S), the MC3000 Laser with Rotating Scan Turret (MC3000R or MC3090R) and the MC3090 Gun (MC3090G). For more information on the Rotating Scan Turret, see *Figure 1-3 on page 1-4*.

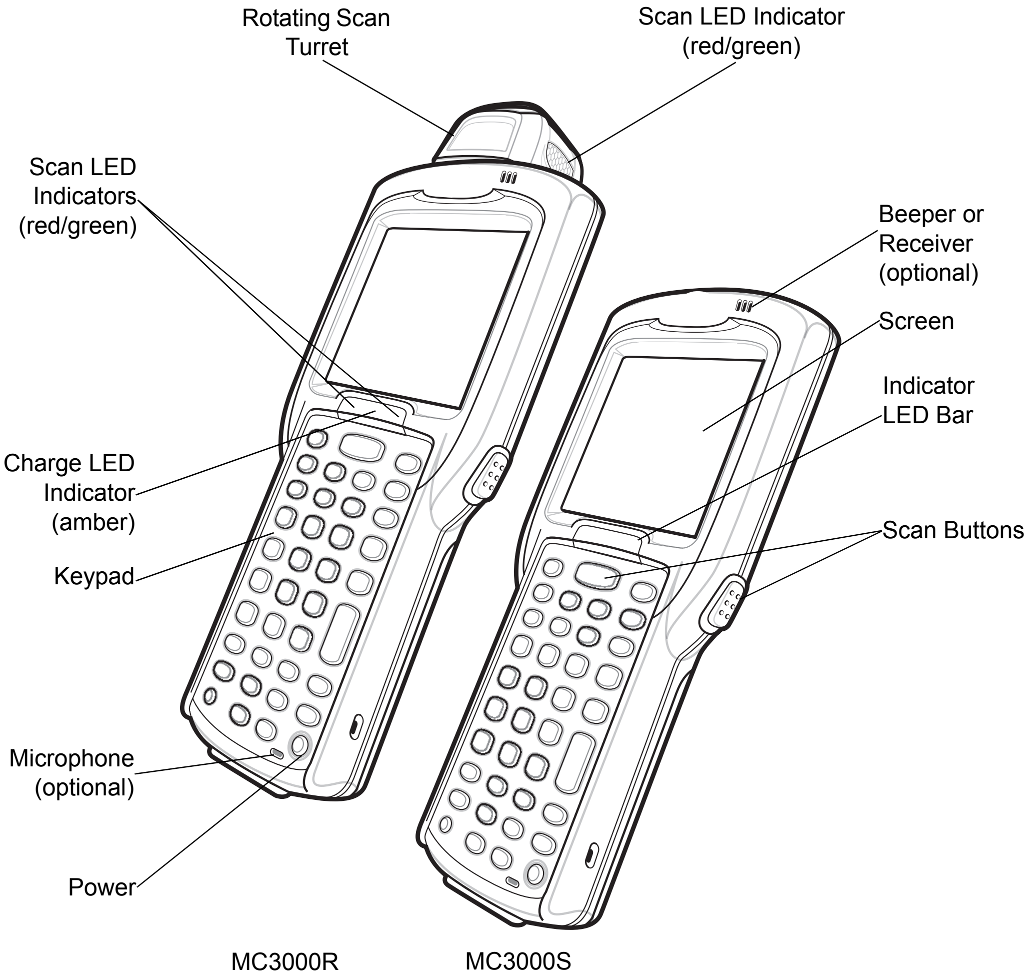

Rotating Scan Turret
Scan LED Indicator (red/green)
Scan LED Indicators (red/green)
Beeper or Receiver (optional)
Screen
Indicator LED Bar
Charge LED Indicator (amber)
Scan Buttons
Keypad
Microphone (optional)
Power
MC3000R
MC3000S

Figure 1-1 *MC3000 Imager (MC3000S) and MC3000 Laser (MC3000R) Mobile Computers (front view)*

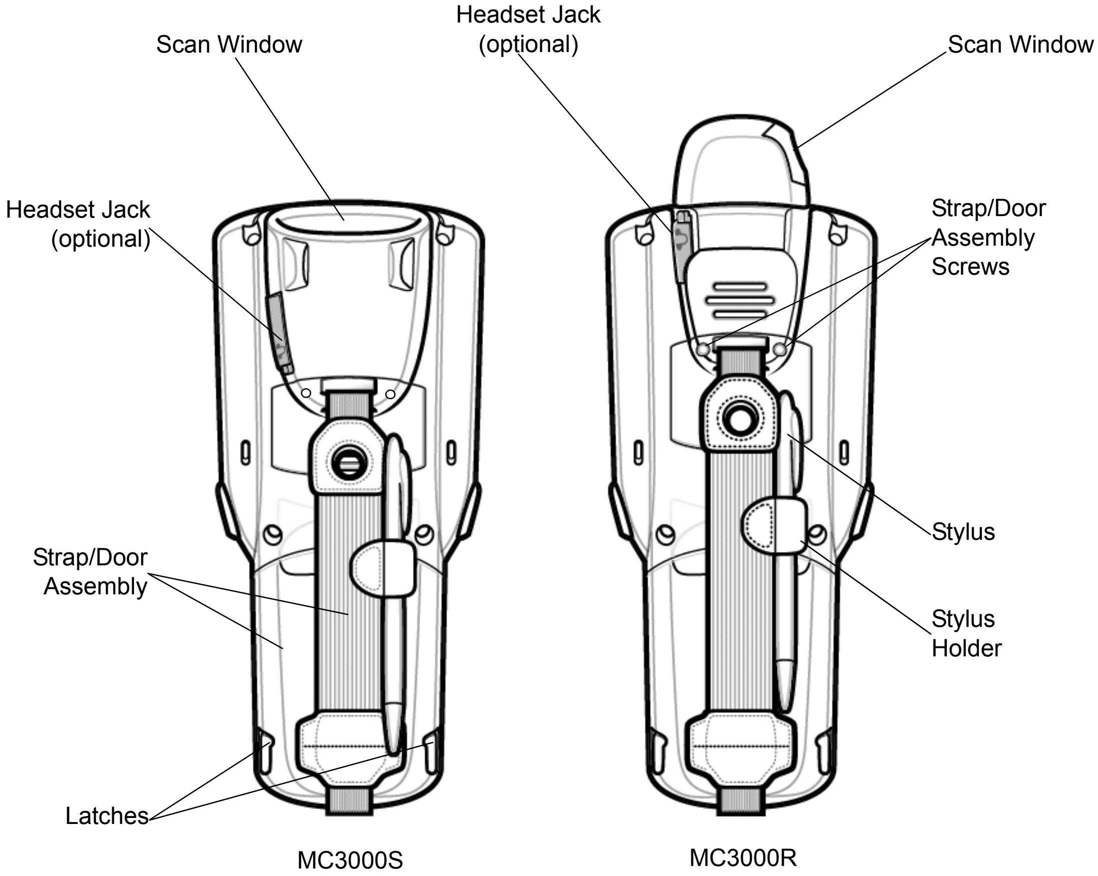


Figure 1-2 *MC3000 Imager (MC3000S) and MC3000 Laser (MC3000R) Mobile Computers (back view)*

Rotating Scan Turret

The MC3000R mobile computer features a Rotating Scan Turret with three position stops. This feature offers greater scanning flexibility.

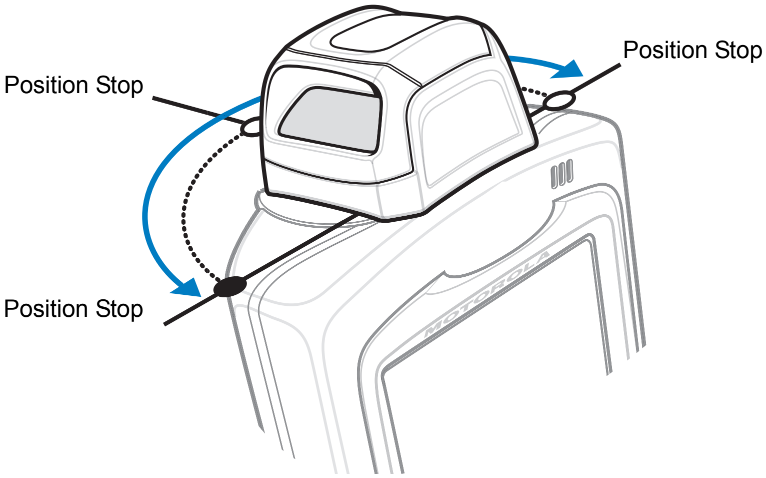


Figure 1-3 *Rotating Scan Turret*

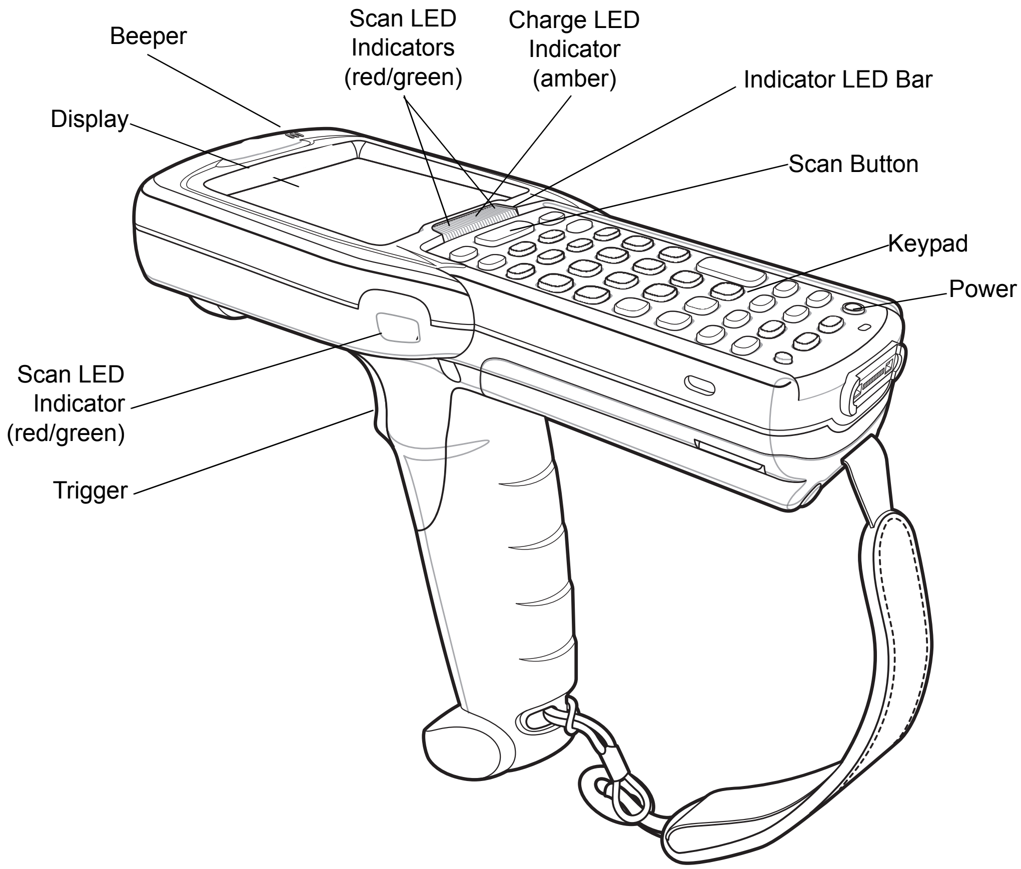

Beeper
Scan LED Indicators (red/green)
Charge LED Indicator (amber)
Indicator LED Bar
Display
Scan Button
Keypad
Power
Scan LED Indicator (red/green)
Trigger

Figure 1-4 *MC3090G Mobile Computer*

Mobile Computer Startup

To start using the mobile computer:

- Install the main battery.
- Charge the main battery and the backup battery.
- Start the mobile computer.

Install Main Battery

If the main battery is charged, the mobile computer can be used immediately. If the main battery is not charged, see *Battery Charging on page 1-8*. To remove the main battery, see *Main Battery Removal on page 1-13*.

To install the main battery:

1. Rotate the latches to the open position.

⚠ ***CAUTION*** Do not lift up on the Latches when removing the Strap/Door Assembly. Lift up on the Hand Strap only.

2. Pull on the strap to lift the Strap/Door Assembly off, bottom first.

⚠ ***CAUTION*** On the MC3090G battery, do not remove the battery pull tab. The pull tab is for enabling easy battery removal from the device.

3. Insert the battery into the slot, bottom first and press the battery gently into the slot. The battery clip locks the battery into place.
4. With the latches in the open position, replace the Strap/Door Assembly, top first and press to close.
5. Rotate the latches (to the lock position) to lock the Strap/Door Assembly in place.

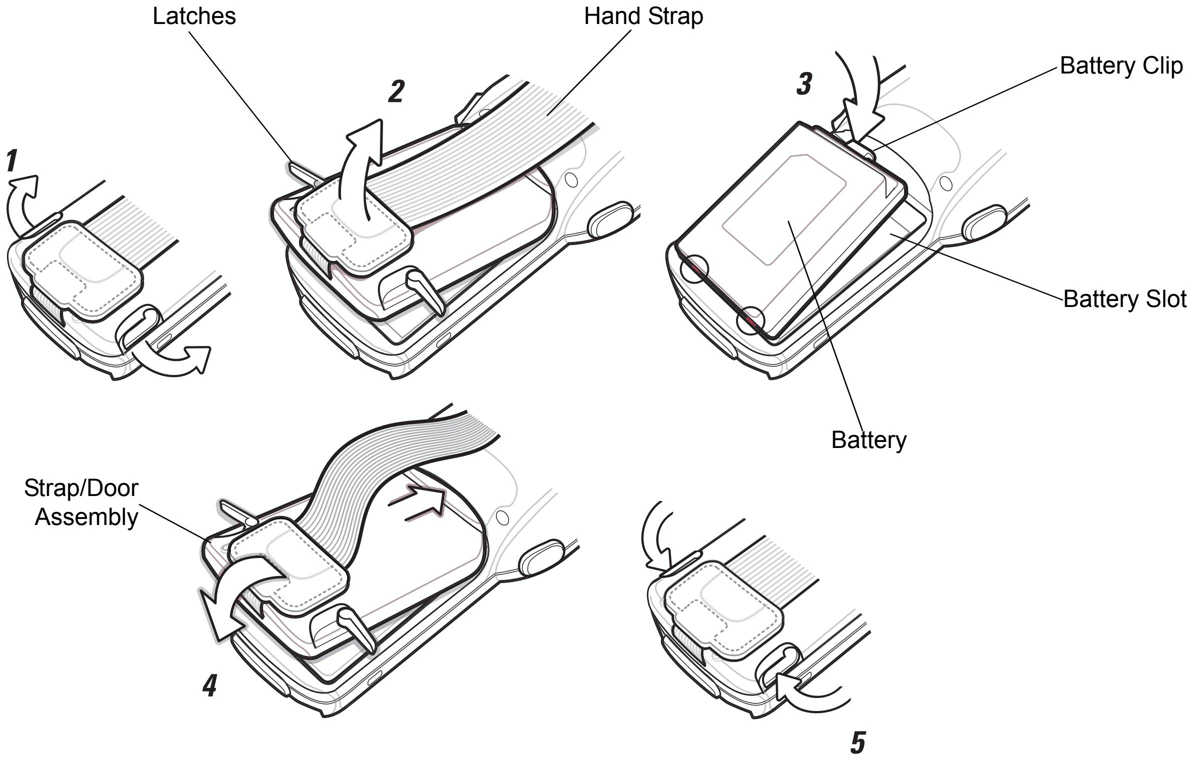


Figure 1-5 *Main Battery Installation*

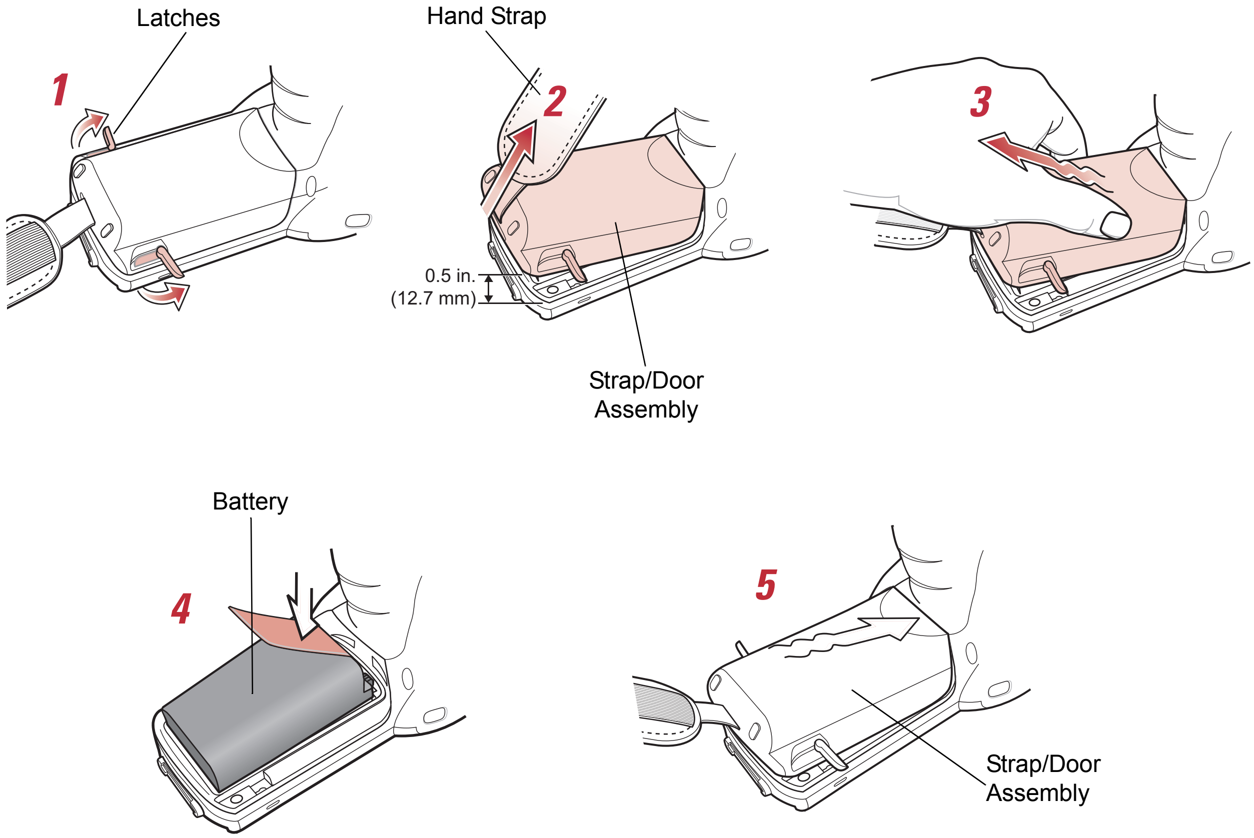


Figure 1-6 *Main Battery Installation (MC3090G)*

Battery Charging

CAUTION Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 8-1*.

Use the mobile computer cradles, cables and spare battery chargers to charge the mobile computer main battery.

The main battery can be charged before insertion into the mobile computer or after it is installed. There are two main batteries for the MC3000, the Standard Battery and the Extended Life Battery. Either battery can be used, but the Extended Life Battery requires a different Strap/Door Assembly. Use one of the spare battery chargers to charge the main battery (out of the mobile computer) or one of the cradles to charge the main battery while it is installed in the mobile computer.

Before using the mobile computer for the first time, fully charge the main battery until the amber Charge LED Indicator remains lit (see *Table 1-2 on page 1-9* for charge status indications). The Standard Battery fully charges in less than four hours and the Extended Life Battery fully charges in less than six hours.

The mobile computer is equipped with a memory backup battery which automatically charges from the main battery whether or not the mobile computer is operating or is in suspend mode. The memory backup battery retains data in memory for at least 30 minutes when the mobile computer's main battery is removed or fully discharged. When the mobile computer 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 mobile computer for 15 hours to ensure that the memory backup battery fully charges. If the main battery is removed from the mobile computer or the main battery is fully discharged, the memory backup battery completely discharges in several hours.

When the main battery reaches a very low battery state, the combination of main battery and backup battery retains data in memory for at least 72 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.

Batteries must be charged within the 32° to 104° F (0° to +40° C) ambient temperature range.

The following accessories can be used to charge the batteries:

- Cradles (and a power supply):
  - Single Slot Serial/USB Cradle
  - Four Slot Cradles.
- Cables (and a power supply):
  - USB Client Charge Cable
  - Serial (RS232) Charge Cable.
- Spare Battery Chargers (and a power supply):
  - Single Slot Serial/USB Cradle
  - Four Slot Spare Battery Charger
  - Universal Battery Charger (UBC) Adapter.

To charge the mobile computer using the cradles:

1. Insert the mobile computer into a cradle. See *Chapter 2, Accessories* for accessory information.

2. The mobile computer starts to charge automatically. The amber Charge LED Indicator indicates the charge status. See *Table 1-2 on page 1-9* for charging indications.

To charge the mobile computer using the cables:

1. Connect the MC3000 Communication/Charge Cable to the appropriate power source and connect to the mobile computer. See *Chapter 2, Accessories* for accessory setup.
2. The mobile computer starts to charge automatically. The amber Charge LED Indicator indicates the charge status. See *Table 1-2 on page 1-9* for charging indications.

Table 1-2 Mobile Computer LED Charge Indicators

LED	Indication
Off	Mobile computer not placed correctly in the cradle; cable not connected correctly; charger is not powered.
Fast Blinking Amber	Error in charging; check placement of the mobile computer.
Slow Blinking Amber	Mobile computer is charging.
Solid Amber	Charging complete. Note: When the battery is initially inserted in the mobile computer, the amber LED flashes once if the battery power is low or the battery is not fully inserted.

Spare Battery Charging

There are three accessories that can be used to charge a spare battery:

- Single Slot Serial/USB Cradle
- Four Slot Spare Battery Charger
- UBC Adapter.

To charge a spare battery:

1. Connect the charging accessory to the appropriate power source. See *Chapter 2, Accessories* for setup instructions.
2. Insert the spare battery into the spare battery charging slot and gently press down on the battery to ensure proper contact.

The battery starts to charge automatically. The charge LED Indicator lights to indicates the charge status. See *Chapter 2, Accessories* for charging indications. The Standard Battery usually fully charges in less than four hours and the Extended Life Battery usually fully charges in less than six hours.

Stylus

Use the stylus to select items and enter information on the screen. The stylus functions as a pen and a mouse. Tap the touch screen once with the stylus to select options and open menu items.

To remove the stylus, slide the stylus out of the stylus holder. To store the stylus, push the stylus back into the stylus holder.

Starting the Mobile Computer

When the mobile computer is powered on for the first time, it initializes. The **Zebra Splash** screen appears for a short period of time, followed by the **Calibration** screen.

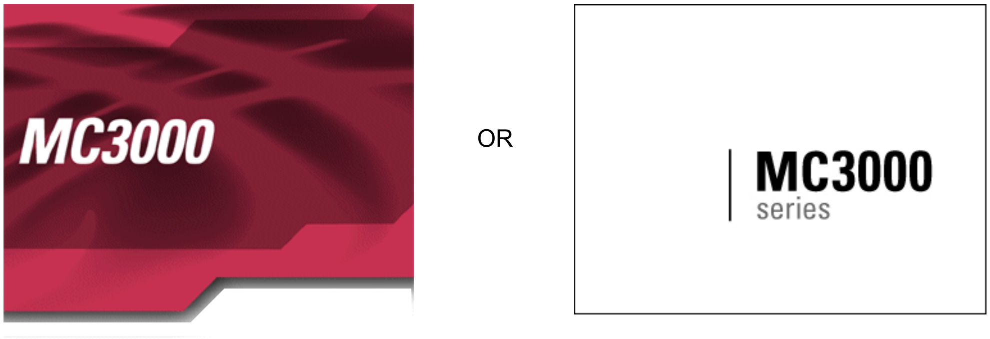


Figure 1-7 *Zebra Splash Screen*

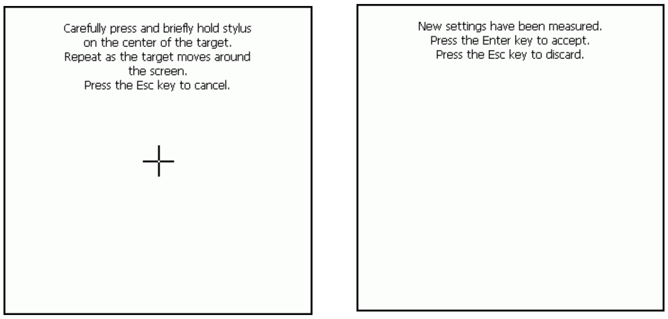
After the calibration procedure is performed the factory default settings launch the **Demo window**. Application specific shells may provide application specific windows instead of the **Demo window**. These screens also appear when a cold boot is performed.

If the mobile computer does not power on, see *Resetting the Mobile Computer on page 1-11*.

Calibration Screen

Use the **Calibration** screen to align the touch screen:

1. Remove the stylus from the stylus holder.
2. Carefully press and briefly hold the tip of stylus on the center of the **Calibration** screen target. Repeat the procedure as the target moves and stops at different locations on the screen. This enters the new calibration settings.



Carefully press and briefly hold stylus
on the center of the target.
Repeat as the target moves around
the screen.
Press the Esc key to cancel.

New settings have been measured.
Press the Enter key to accept.
Press the Esc key to discard.

Calibration Screen

Confirm Calibration
Resave Screen

Figure 1-8 *Calibration Screen*

3. Once all of the new calibration settings are input, the **Confirm Calibration Resave** screen appears. Tap the screen within 30 seconds to save the new calibration settings or allow the 30 second timer to expire and the new calibration settings are not saved.

Demo Window

The **Demo window** is the factory default menu. On initial power up (or on a warm or cold boot) the **Demo window** appears. These sample/demo applications are intended to be used by application developers as application development examples. These applications were not developed to support end users. Refer to the *Zebra Application Guide* for information about the **Demo window** applications.

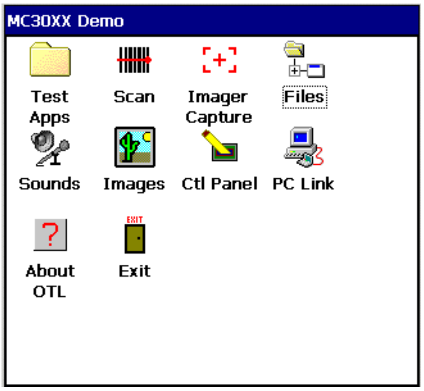


Figure 1-9 *Demo Window*

Resetting the Mobile Computer

Windows CE Devices

If the mobile computer stops responding to input, reset it. There are two reset functions, warm boot and cold boot. A warm boot restarts the mobile computer by closing all running programs. All data that is not saved is lost.

A cold boot also restarts the mobile computer, but erases all stored records and entries from RAM. In addition it returns formats, preferences and other settings to the factory default settings.

Perform a warm boot first. If the mobile computer still does not respond, perform a cold boot.

Performing a Warm Boot

To perform a warm boot on 28, 38 and 48-key keypad configurations:

1. Press and simultaneously hold **7**, **9** and **Power**. Do not hold down any other keys or buttons.
2. As the mobile computer initializes MC3000 demo window appears.

CAUTION Files that remain open during a warm boot may not be retained.

To perform a warm boot on 20-key keypad configurations:

1. Press and simultaneously hold the **7** and **9** keys and the press the **MENU** and **Fn** keys. Do not hold down any other keys or buttons.
2. As the mobile computer initializes MC3000 demo window appears.

CAUTION Files that remain open during a warm boot may not be retained.

Performing a Cold Boot

A cold boot restarts the mobile computer and erases all user stored records and entries from RAM. *Never perform a cold boot unless a warm boot does not solve the problem.*

CAUTION Cold boot resets the mobile computer, to the default settings. All added applications and all stored data are removed. Do not cold boot without support desk approval.

To perform a cold boot 28, 38 and 48-key keypad configurations:

1. Simultaneously press and then release the **1**, **9** and **Power** keys. Do not hold down any other keys or buttons. As the mobile computer initializes, the Zebra splash window, *Figure 1-7 on page 1-9*, appears for about a minute.
2. Calibrate the touch screen. See *Calibration Screen on page 1-10* to calibrate the mobile computer screen.

To perform a cold boot on 20-key keypad configurations:

1. Simultaneously press and then release the **1** and **9, MENU** and **Fn** keys. Do not hold down any other keys or buttons. As the mobile computer initializes, the Zebra splash window, *Figure 1-7 on page 1-9*, appears for about a minute.
2. Calibrate the touch screen. See *Calibration Screen on page 1-10* to calibrate the mobile computer screen.

Windows Mobile 6.1 Devices

There are two reset functions, warm boot and cold boot.

- A warm boot restarts the mobile computer and closes all running programs.
- A cold boot also restarts the mobile computer and closes all running programs but also resets the Real-Time-Clock (RTC).

Data saved in flash memory or a memory card is not lost. Perform a warm boot first. This restarts the mobile computer and saves all *stored* records and entries. If the mobile computer still does not respond, perform a cold boot.

Performing a Warm Boot

To perform a warm boot on 28, 38 and 48-key keypad configurations:

1. Press and simultaneously hold **7**, **9** and **Power**. Do not hold down any other keys or buttons.
2. As the mobile computer initializes Today screen appears.

Performing a Cold Boot

A cold boot restarts the mobile computer. The operating system and all applications are restarted. File storage is preserved. The Real-Time-Clock (RTC) resets. *Only perform a cold boot if a warm boot does not solve the problem.*

1. To perform a cold boot 28, 38 and 48-key keypad configurations, simultaneously press and then release the **1**, **9** and **Power** keys. Do not hold down any other keys or buttons.
2. As the mobile computer initializes, the splash window, *Figure 1-7 on page 1-9*, appears for about a minute.

Waking the Mobile Computer

The wakeup conditions define what actions wake up the mobile computer after it has gone into suspend mode. The mobile computer can go into suspend mode by either pressing the Power button or automatically by Control Panel time-out settings. These settings are configurable and the factory default settings are shown in *Table 1-3*.

Table 1-3 Wakeup Default Settings

Condition for Wakeup	Power Button	Automatic Time-out
AC power is applied.	No	Yes
Mobile computer is inserted into a cradle.	No	Yes
Mobile computer is removed from a cradle.	No	Yes
Mobile computer is connected to a serial device.	No	Yes
Mobile computer is connected to a USB device.	No	Yes
Mobile computer is disconnected from a USB device.	No	Yes
A key is pressed.	No	Yes
The scan triggered is pressed.	No	Yes
The screen is touched.	No	No
Wireless LAN activity is detected.	No	No

Main Battery Removal

Before removing the main battery, turn off the mobile computer.

To remove the main battery:

1. Rotate the latches to the open position.

CAUTION Do not lift up on the Latches when removing the Strap/Door Assembly. Lift up on the Hand Strap only.

2. Lift the Hand Strap to lift the Strap/Door Assembly off, bottom first.

CAUTION On the MC3090G battery, do not remove the battery pull tab. The pull tab is for enabling easy battery removal from the device.

3. Release battery:
   a. On the MC3000S/R, release the battery clip (at the top of the battery) and lift the battery out top first.
   b. On the MC3090G, pull the battery pull tab to unclip the battery and lift the battery out top first. If the battery does not have a pull tab, use the stylus to unclip the battery and then lift the battery.

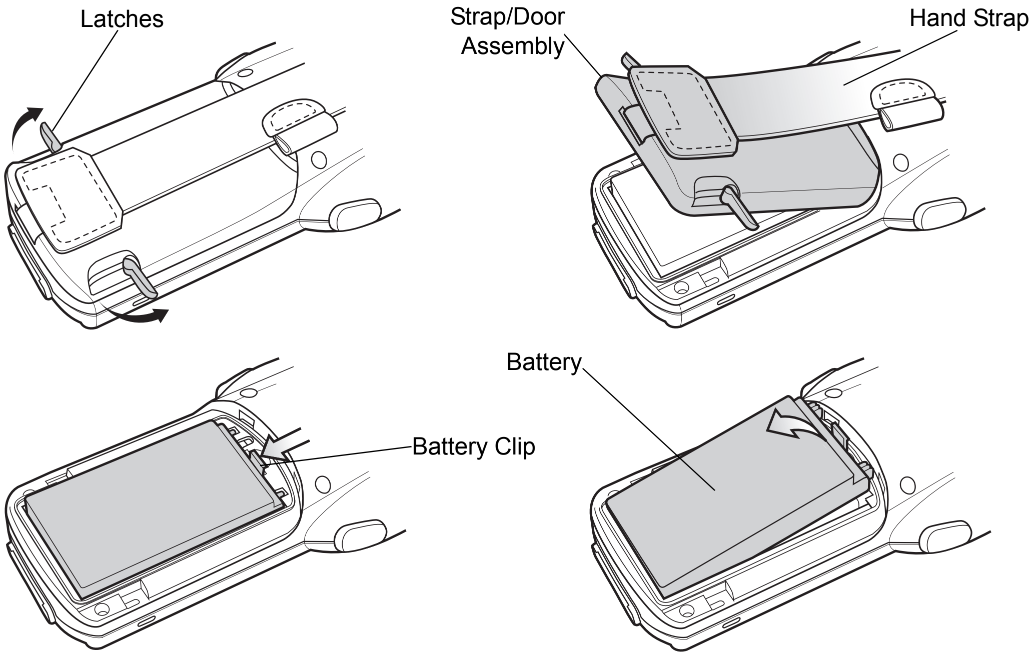


Figure 1-10 *Main Battery Removal (MC3000S/R)*

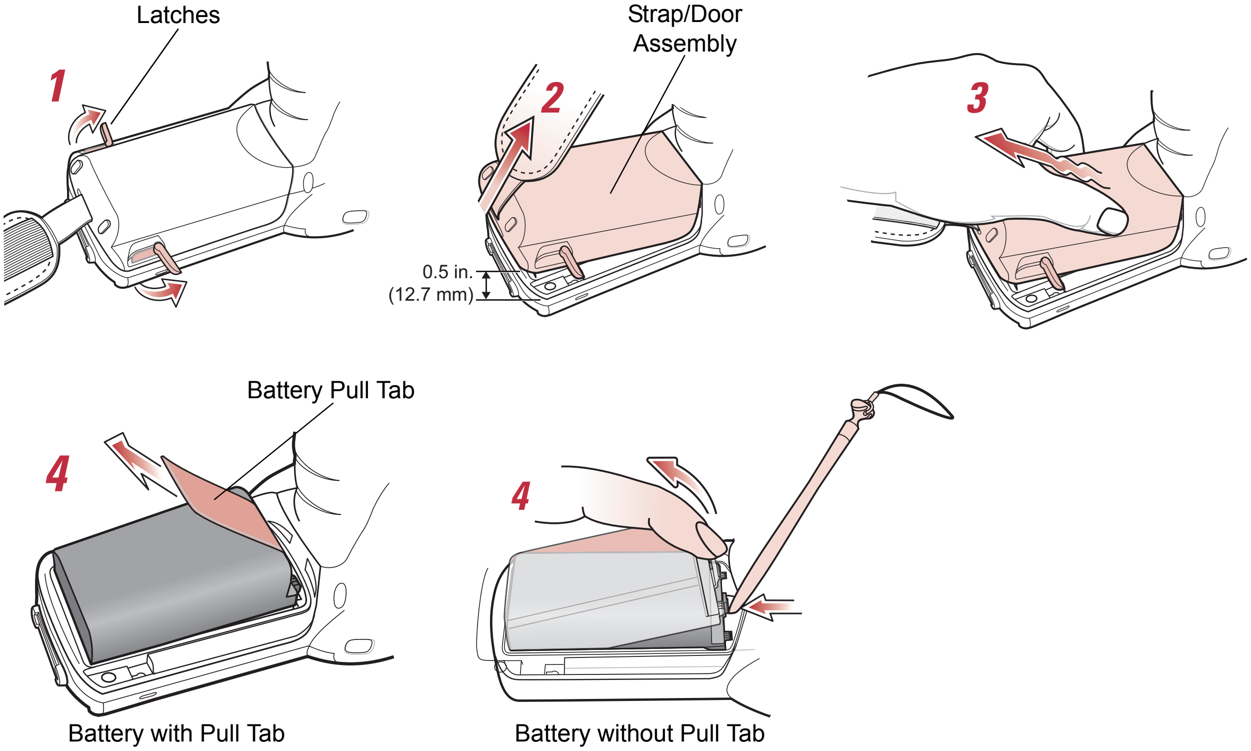


Figure 1-11 *Main Battery Removal (MC3090G)*

Strap/Door Assembly Removal and Replacement

The Strap/Door Assembly consists of a hand strap and the battery door. There are two versions of this assembly, one for the Standard Battery and one for the Extended Life Battery. Before removing the Strap/Door Assembly, press the red **Power** button to turn off the screen and set the mobile computer to suspend mode.

To remove the Strap/Door Assembly:

1. Rotate the latches to the open position.

CAUTION Do not lift up on the Latches when removing the Strap/Door Assembly. Lift up on the Hand Strap only.

2. Lift the Hand Strap to lift the Strap/Door Assembly off, bottom first.
3. Use a #00 Phillips screwdriver to remove the screws.
4. Lift the mounting clip.
5. Slide the mounting clip out of the strap loop.

Reverse the procedure to replace the Strap/Door Assembly.

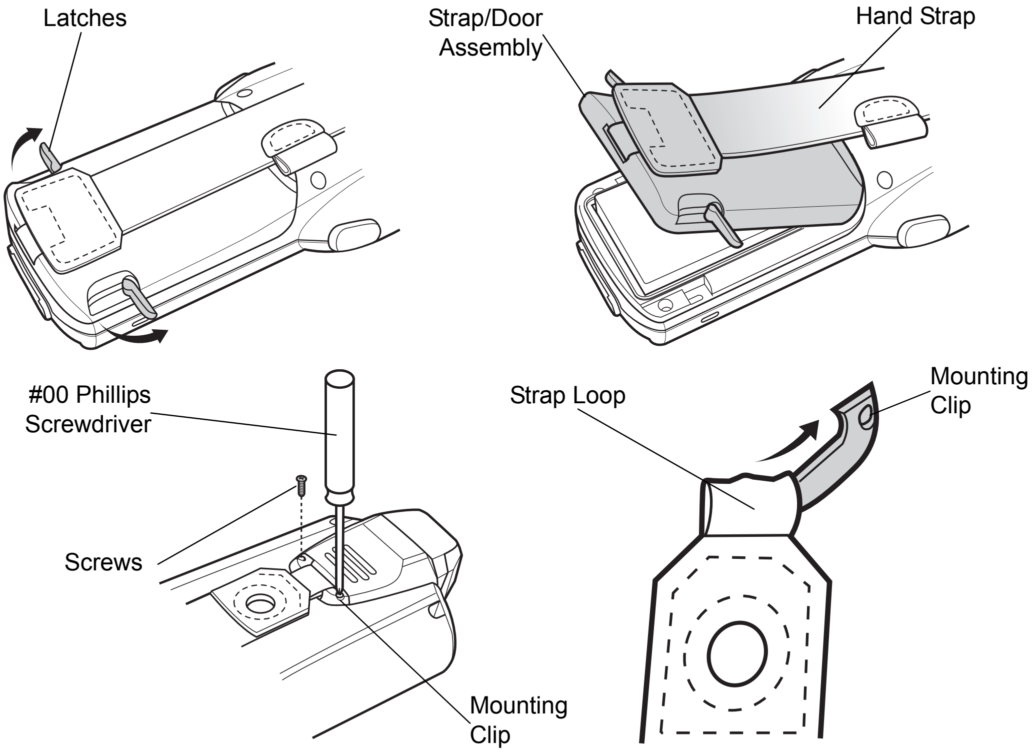


Figure 1-12 *Strap/Door Removal and Replacement*

Strap/Door Assembly Removal and Replacement (MC3090G)

The Strap/Door Assembly consists of a hand strap and the battery door. Before removing the Strap/Door Assembly, press the red **Power** button to turn off the screen and set the mobile computer to suspend mode.

To remove the Strap/Door Assembly:

1. Slip the button through the loop.
2. Remove loop section from handle.
3. Rotate the latches to the open position.

CAUTION Do not lift up on the latches when removing the Strap/Door Assembly. Lift up on the Hand Strap only.

4. Lift the Hand Strap to lift the Strap/Door Assembly off, bottom first.

Reverse the procedure to replace the Strap/Door Assembly.

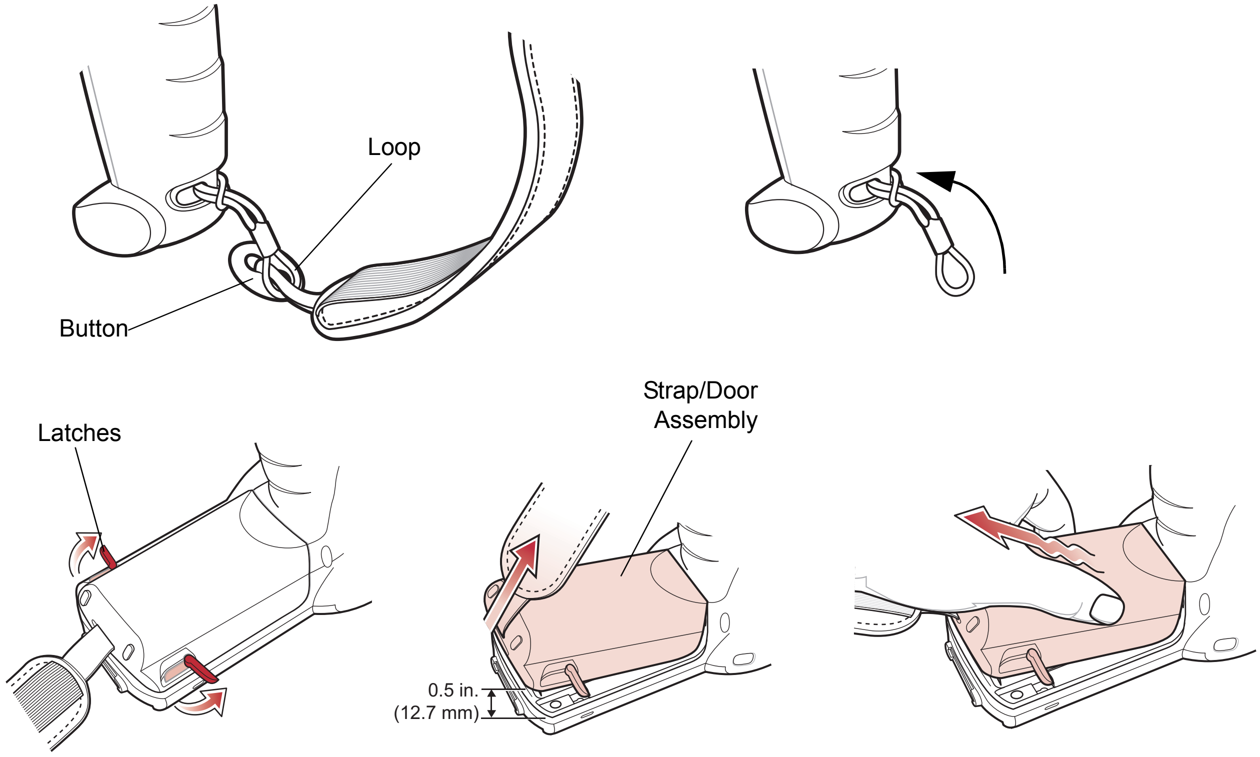
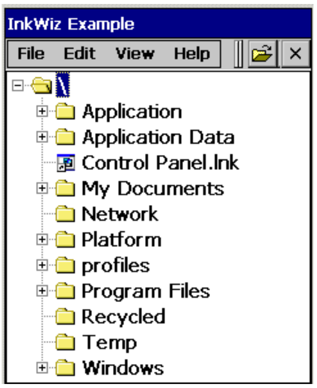


Figure 1-13 *Strap/Door Removal and Replacement (MC3090G)*

File System Directory Structure

The mobile computer directory structure displays all of the file folders. The pre-installed folders are in flash file system memory and optional removable storage devices (SD storage cards).



```
\
  Application
  Application Data
  Control Panel.lnk
  My Documents
  Network
  Platform
  profiles
  Program Files
  Recycled
  Temp
  Windows
```

Figure 1-14 *Mobile Computer Directory Structure*

- **Application** and **Platform** folders are located in flash file system memory.
- The **Windows**, **Program Files**, **profiles**, and **My Documents** folders are composites, RAM based folders generated from ROM.
- The **Network** folder is a link to file systems mapped using the network re-director. The files do not physically reside on the mobile computer.
- The **Temp** and **Recycled** folders typically contain RAM based files.

✓ ***NOTE*** All files copied to the RAM based folders are lost after a cold boot.

Flash Storage

In addition to the RAM based storage the mobile computer 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. See *Flash Storage on page 6-16* for a detailed discussion.

Launching Applications

The **Application/Startup** folder is used to launch programs automatically when the mobile computer is powered on or after a warm or cold boot.

✓ ***NOTE*** The **Windows/Startup** folder is not supported.

There are two ways to launch programs automatically:

1. Place the executable in the **Startup** folder (located in the **Application** folder).
2. Place a .run file in the **Startup** folder. A .run file is a simple text file that contains the path to an application as well as the name of the application to run.

Refer to the *SMDK Help File* included with the SMDK for more information on the **Startup** folder.

Chapter 2 Accessories

Introduction

The MC3000 accessories provide a variety of product support capabilities. Accessories include cradles, cables, spare battery chargers and SD cards.

Cradles

- Single Slot Serial/USB cradle charges the mobile computer main battery and/or a spare battery. It also synchronizes the mobile computer with a host computer through either a serial or a USB connection.
- Four Slot Charge Only cradle charges up to four mobile computers.
- Four Slot Ethernet cradle charges up to four mobile computers and provides Ethernet communication capability.

Spare Battery Chargers

- Four Slot Spare Battery Charger charges up to four MC3000 spare batteries.
- UBC Adapter adapts the UBC2000 for use with the MC3000 spare batteries.

Cables

The cables snap on to the mobile computer and are used to connect external devices to the mobile computer.

- USB client charge cable
- Serial (RS232) charge cable
- O’Neil printer cable (provided by O’Neil)
- Zebra printer cable (provided by Zebra)
- Monarch printer cable (provided by Monarch).

SD Card

The SD card provides additional storage capacity for the mobile computer.

Single Slot Serial/USB Cradle

CAUTION Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 8-1*.

This section describes how to set up and use the Single Slot Serial/USB cradle. For cradle setup, see *Figure 2-2*. For communications setup procedures, see *USB Connection Setup on page 2-34* and/or *Serial Communication Setup on page 2-30*.

The Single Slot Serial/USB cradle:

- Provides 5.4VDC power for operating the mobile computer, charging the battery and charging a spare battery.
- Provides a serial port and a USB port (mini AB receptacle) for data communication between the mobile computer and a host computer or other serial devices (e.g., a printer).
- Synchronizes information between the mobile computer and a host computer. With customized or third party software, it can also synchronize the mobile computer with corporate databases.
- Provides serial connection through the serial pass-through port for communication with a serial device, such as a host computer. For communication setup procedures, see *Serial Communication Setup on page 2-30*.
- Provides USB connection through the USB pass-through port for communication with a USB device, such as a host computer. For communication setup procedures, see *USB Connection Setup on page 2-34*.

CAUTION Use only a Zebra 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. See the MC3000 User Guide for the power supply regulatory compliance statement.

Setup

✓ ***NOTE*** The cradle requires a dedicated port on the host computer. Select either serial or USB for communications, do not connect the cradle to both serial and USB ports.

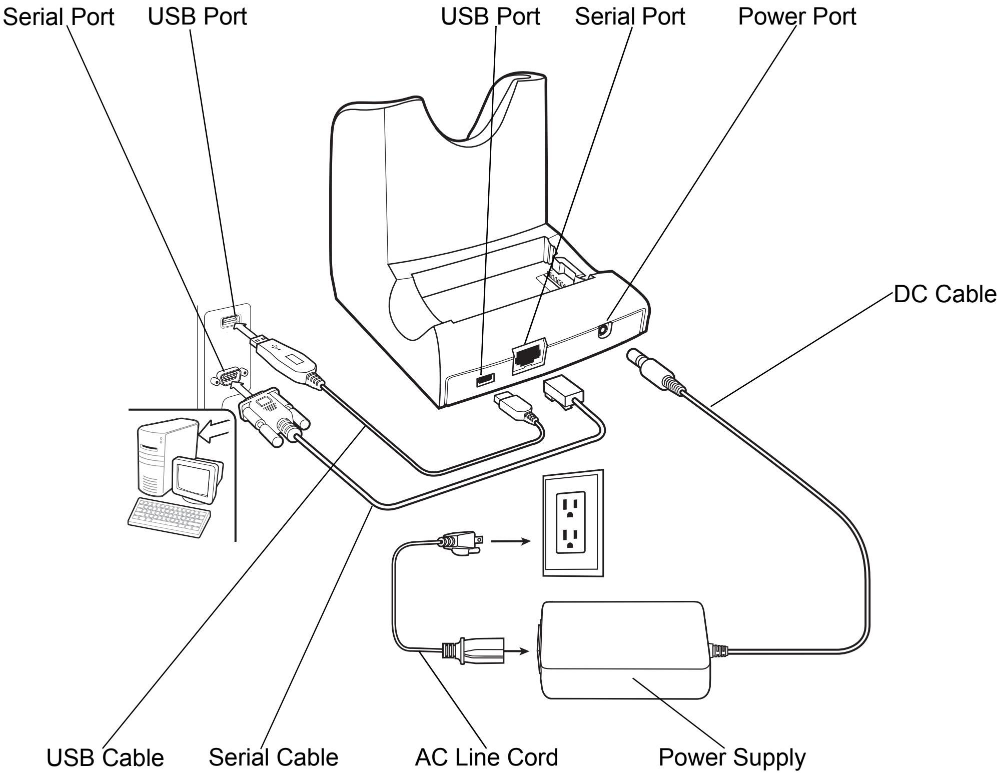


Figure 2-1 *Single Slot Serial/USB Cradle Setup*

Battery Charging

The Single Slot Serial/USB cradle can charge the mobile computer main battery and a spare battery simultaneously.

To charge the mobile computer:

1. Connect the Single Slot Serial/USB cradle to a Zebra approved power source.
2. Slide the mobile computer into the mobile computer slot. The amber Charge LED Indicator indicates the mobile computer battery charging status. The Standard Battery charges in less than four hours and the Extended Life Battery charges in less than six hours. See *Table 2-1* for charging status indications.

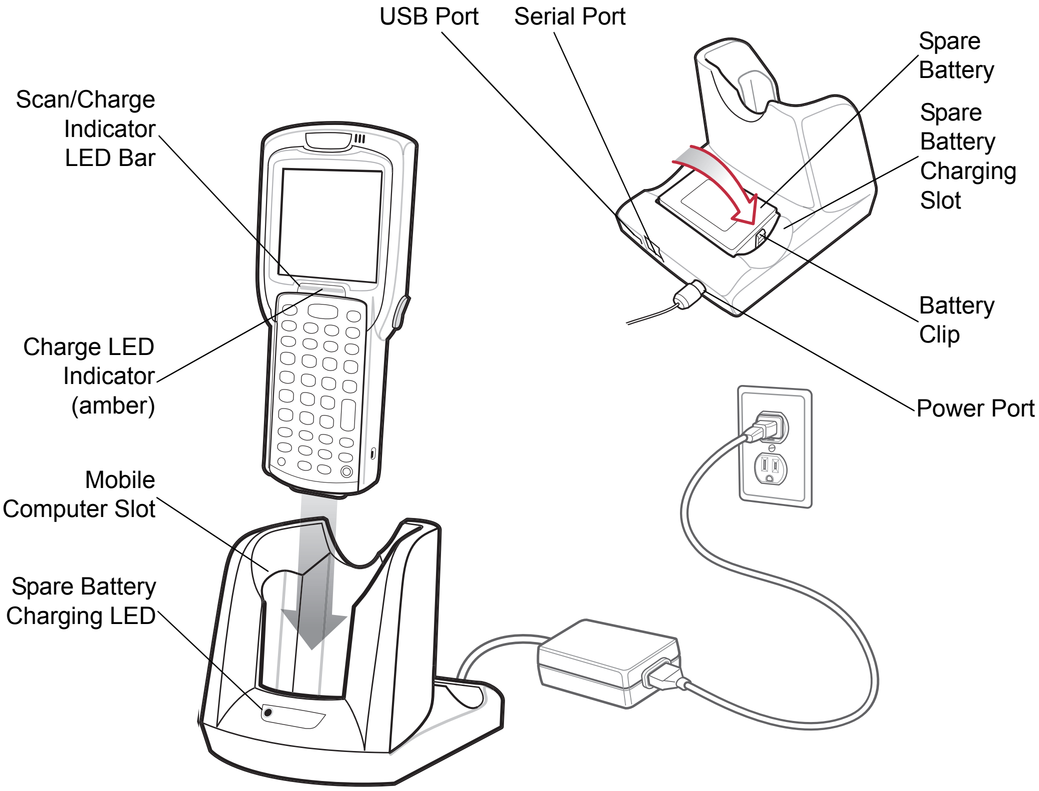

USB Port
Serial Port
Spare Battery
Scan/Charge Indicator LED Bar
Spare Battery Charging Slot
Battery Clip
Charge LED Indicator (amber)
Power Port
Mobile Computer Slot
Spare Battery Charging LED

Figure 2-2 *Single Slot Serial/USB Cradle*

3. When charging is complete, remove the mobile computer from the mobile computer slot.

To charge a spare battery:

1. Connect the Single Slot Serial/USB cradle to a Zebra approved power source.
2. Insert the spare battery into the spare battery charging slot, bottom first, and pivot the top of the battery down onto the contact pins.
3. Gently press down on the battery to ensure proper contact.
4. The cradle Spare Battery Charging LED indicates the spare battery charging status. The Standard Battery usually charges in less than four hours and the Extended Life Battery usually charges in less than six hours. See *Table 2-1* for charging status indications.
5. When charging is complete, press the battery clip and lift the battery out of the slot.

LED Charge Indications

The Single Slot Serial/USB cradle uses the amber Charge LED Indicator to indicate MC3000 battery charging status and the Spare Battery Charging LED to indicate spare battery charging status. See *Table 2-1* for charging status indications.

Table 2-1 *LED Charging Status Indicators*

LED	Indication
Mobile Computer Charging (LED on mobile computer)	
Off	Mobile computer not placed correctly in the cradle; cable not connected correctly; charger is not powered.
Fast Blinking Amber	Error in charging; check placement of mobile computer.
Slow Blinking Amber	Mobile computer is charging.
Solid Amber	Charging complete. Note: When the battery is initially inserted in the mobile computer, the amber LED flashes once if the battery power is low or the battery is not fully inserted.
Spare Battery Charging (LED on cradle)	
Off	No spare battery in slot; spare battery not placed correctly; cradle is not powered.
Fast Blinking Amber	Error in charging; check placement of spare battery.
Slow Blinking Amber	Spare battery is charging.
Solid Amber	Charging complete.

Communication Setup

To connect the Single Slot Serial/USB cradle to a serial or USB device:

1. Connect Single Slot Serial/USB cradle cable to the communications port.
2. Slide the mobile computer into the mobile computer slot. The amber Charge LED Indicator indicates the mobile computer battery charging status and that the mobile computer is seated in the cradle. For more information on communications setup procedures, see *USB Connection Setup on page 2-34* and/or *Serial Communication Setup on page 2-30*.

Four Slot Charge Only Cradle

CAUTION Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 8-1*.

The Four Slot Charge Only cradle:

- Provides 5.4VDC power for operating the mobile computer and charging the battery.
- Simultaneously charges up to four mobile computers.

CAUTION Use only a Zebra 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 MC3000 User Guide for the power supply regulatory compliance statement.

Setup

Connect the Four Slot Charge Only cradle to a Zebra approved power source.

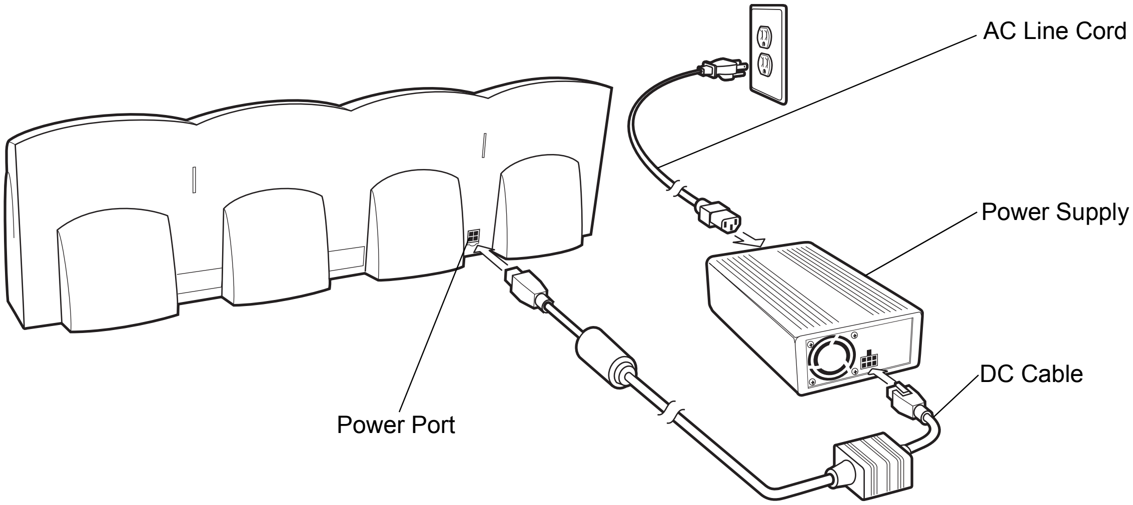


Figure 2-3 *Four Slot Charge Only Cradle, Setup*

Battery Charging

The Four Slot Charge Only cradle can charge up to four mobile computers simultaneously.

To charge the mobile computer:

1. Connect the Four Slot Charge Only cradle to a Zebra approved power source.
2. Slide the mobile computer into the mobile computer slot.

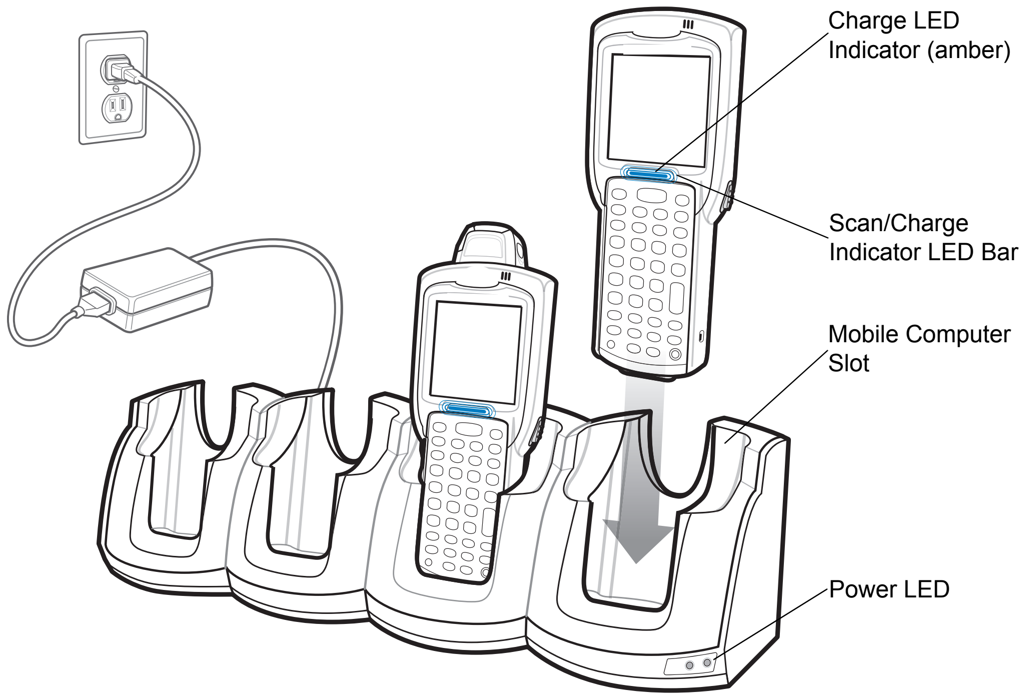


Figure 2-4 *Four Slot Charge Only Cradle*

3. The mobile computer amber Charge LED Indicator indicates the mobile computer battery charging status. The Standard Battery usually charges in less than four hours and the Extended Life Battery usually charges in less than six hours. See *Table 2-1 on page 2-5* for charging status indications.

4. When charging is complete, remove the mobile computer from the cradle.

Power LED

The green Power LED lights to indicate that the Four Slot Charge Only cradle is connected to a power source.

LED Charge Indications

The Four Slot Charge Only cradle uses the amber Charge LED Indicator to indicate battery charging status. See *Table 2-1 on page 2-5* for charging status indications.

Four Slot Ethernet Cradle

CAUTION Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 8-1*.

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

The Four Slot Ethernet cradle:

- Provides 5.4 VDC power for operating the mobile computer.
- Connects the mobile computer (up to four) to an Ethernet network.

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

CAUTION Use only a Zebra 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 MC3000 User Guide for the power supply regulatory compliance statement.

Setup

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 a Zebra approved power supply.

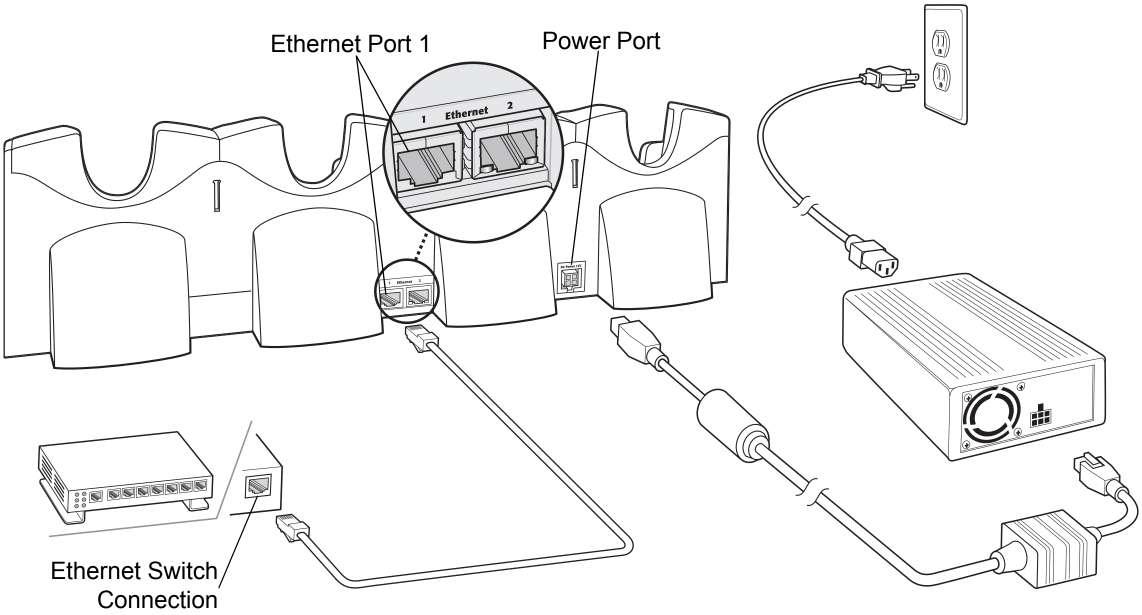


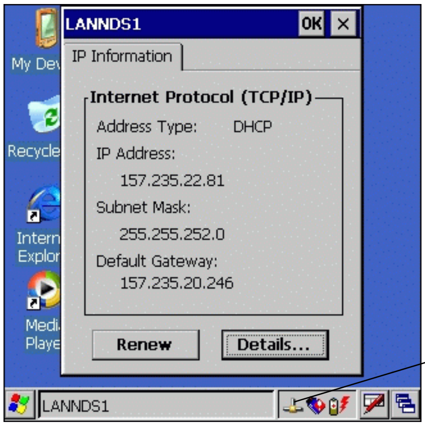
Figure 2-5 *Four Slot Ethernet Cradle Connection*

Ethernet Cradle Drivers (Windows CE 5.0)

The Ethernet cradle drivers are pre-installed on the MC3000 and initiate automatically when the MC3000 is placed in a properly connected Four Slot Ethernet cradle.

When the mobile computer is inserted into the Four Slot Ethernet cradle, the LAN icon indicates that the mobile computer is connected to a network.

Double-tap the **LAN** icon to open the **LANNDS1** window. This window display the TCP/IP information for the mobile computer.



Internet Protocol (TCP/IP)
Address Type: DHCP
IP Address: 157.235.22.81
Subnet Mask: 255.255.252.0
Default Gateway: 157.235.20.246

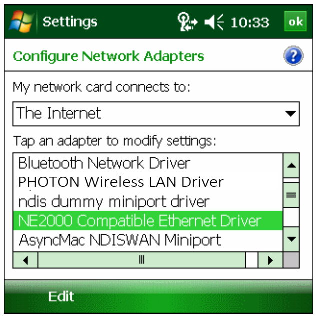
LAN Icon

Figure 2-6 *LANNDS1 Window*

Ethernet Cradle Drivers (Windows Mobile 6.1)

The MC3000 includes Ethernet cradle drivers that initiate automatically when you place the MC3000 in a properly connected Four Slot Ethernet cradle. After inserting the MC3000, configure the Ethernet connection:

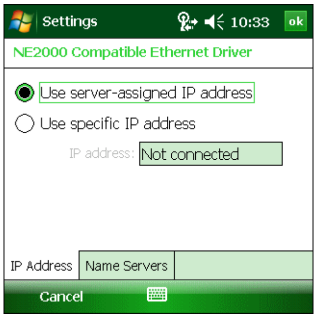
1. Tap **Start** > **Settings** > **Connections** tab >**WiFi** icon. The **Configure Network Adapters** window appears.



My network card connects to:
The Internet
Tap an adapter to modify settings:
Bluetooth Network Driver
PHOTON Wireless LAN Driver
ndis dummy miniport driver
NE2000 Compatible Ethernet Driver
AsyncMac NDISWAN Miniport

Figure 2-7 *Configure Network Adapters Window*

2. In the **My network card connects to:** drop-down list, select the appropriate connection.
3. In the **Tap an adapter to modify settings:** list, select **NE2000 Compatible Ethernet Driver**.



● Use server-assigned IP address
○ Use specific IP address
IP address: Not connected

Figure 2-8 *IP Address Tab*

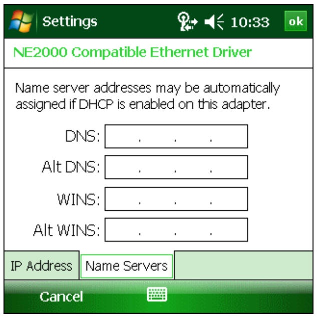
4. In the **IP address** window, select the appropriate radio button:

- **Use server-assigned IP address**

  or

- **Use specific IP address.** Enter the IP address, Subnet mask, and Default gateway, as needed.

5. Tap the **Name Servers** tab.



Settings 10:33 ok

NE2000 Compatible Ethernet Driver

Name server addresses may be automatically assigned if DHCP is enabled on this adapter.

DNS: . . .

Alt DNS: . . .

WINS: . . .

Alt WINS: . . .

Figure 2-9 *Name Servers Tab*

6. Enter the appropriate DNS, Alt DNS, WINS, and Alt WINS server addresses.

7. Tap **ok**.

8. Tap **ok** to exit.

Charging and Communication

Insert the mobile computer into a slot to begin charging and initiate communication.

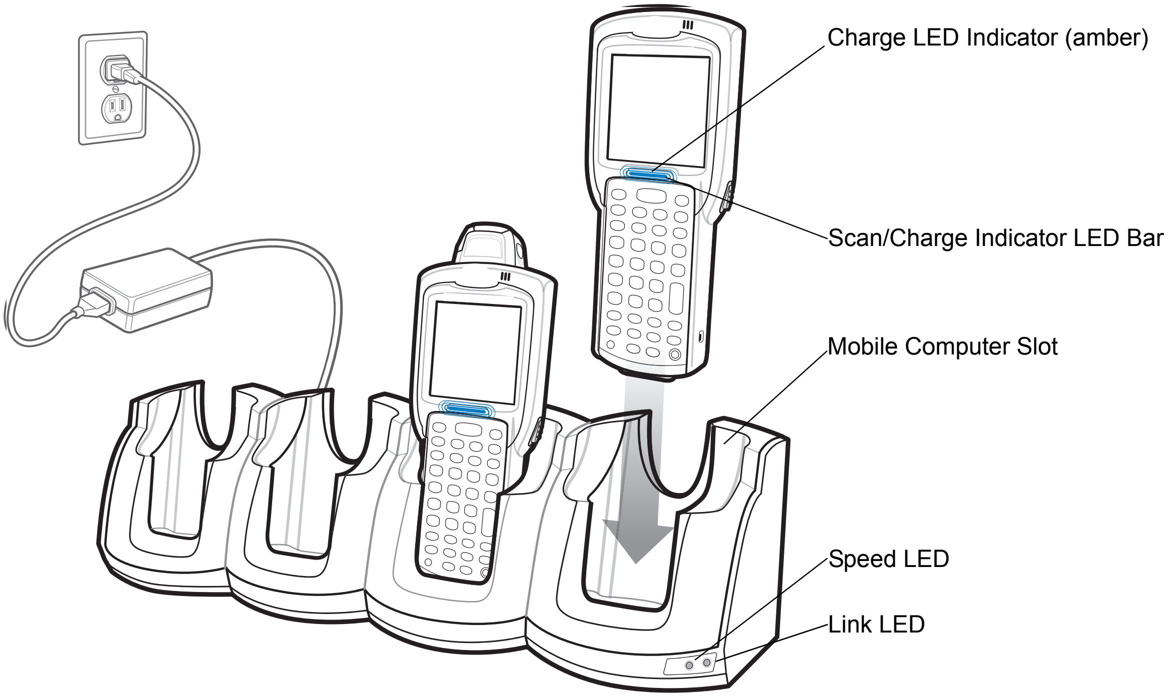


Figure 2-10 *Four Slot Ethernet Cradle*

LED Charge Indications

The charge LED shows the status of the battery charging in the mobile computer. The Standard Battery usually charges in less than four hours and the Extended Life Battery usually charges in less than six hours. See *Table 2-1 on page 2-5* for charging status indications.

Speed LED

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

Daisychaining Ethernet Cradles

To connect several cradles to an Ethernet network, up to four (recommended maximum) Ethernet cradles may be daisychained. 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 daisychain cradles:

1. Connect the first Ethernet cradle to power and to the Ethernet Switch as shown on *Figure 2-5 on page 2-8*.
2. Connect power to the second Ethernet cradle.
3. Connect the daisychain 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. See *Table 2-2* for bandwidth limitations.

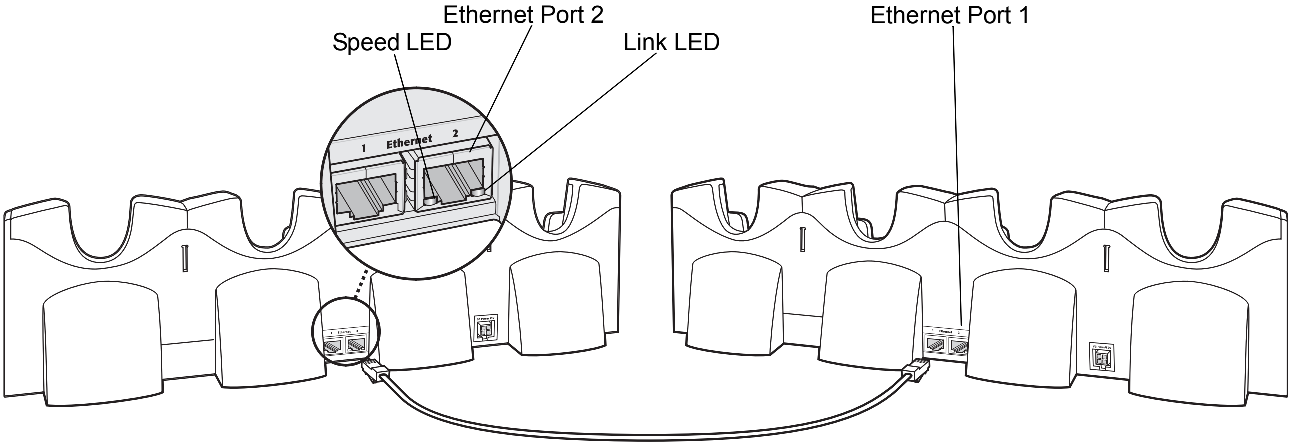


Figure 2-11 *Daisychaining Four Slot Ethernet Cradles*

Bandwidth Considerations when Daisychaining

Each cradle added to the daisychain impacts the bandwidth allocated to each of the inserted mobile computers, particularly when the mobile computers attempt to send and receive at data rates that exceed the bandwidth provided to the chain (typically 100 Mbps). If a mobile computer in a daisychained cradle does not use its bandwidth, that bandwidth is available to other inserted mobile computers.

Table 2-2 shows allocated bandwidth (based on 100 Mbps) for the number of daisychained cradles, with each mobile computer attempting transmission at the maximum data rate.

Table 2-2 *Daisychaining Bandwidth*

Daisychained Ethernet Cradles	Bandwidth Allocation For Each Ethernet Cradle (bits/sec)	Bandwidth Allocation For Each Mobile Computer (bits/sec)
Cradle 1	100,000,000	20,000,000*
Cradle 2	20,000,000	4,000,000
Cradle 3	4,000,000	800,000
Cradle 4	800,000	160,000
Cradle 5**	160,000	32,000
Cradle 6**	32,000	6,400
Cradle 7**	6,400	1,280

* The maximum bandwidth capacity for the mobile computer is 12,000,000 bits/sec.
** Depending on the application, allocated bandwidth may not be adequate.

Wall Mount Bracket

Use the optional Wall Mount Bracket to mount a four slot cradle directly to a wall. To attach the Wall Mount Bracket:

1. Use the Wall Mount Bracket as a template and mark the locations of the four mounting screws.

✓ ***NOTE*** Use fasteners appropriate for the type of wall and the Wall Mount Bracket, mounting slots. The Wall Mount Bracket, mounting slots are designed for a fastener with a #8 pan head.

2. Mount the fasteners to the wall. The screw heads should protrude about a half of an inch from the wall.
3. Slip the Wall Mount Bracket over the screw heads and slide the Wall Mount Bracket down over the screw heads.
4. Tighten the screws to secure the Wall Mount Bracket to the wall.

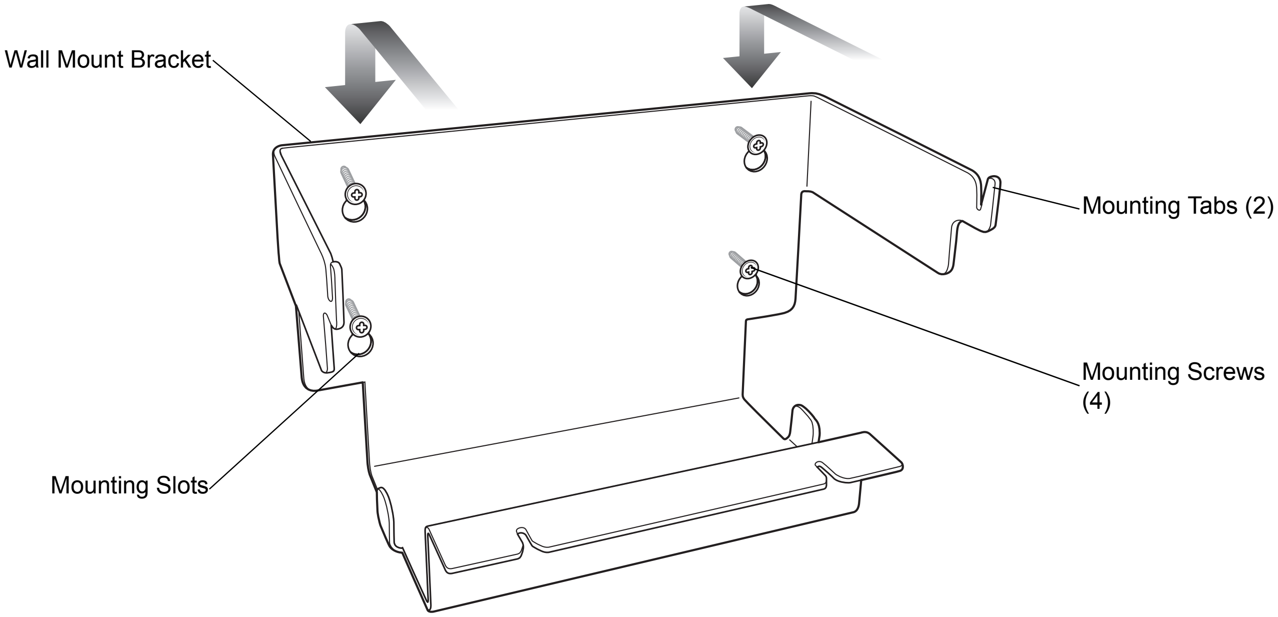


Figure 2-12 *Wall Mount Bracket*

To mount a four slot cradle:

1. Screw the supplied fasteners into the bottom of the four slot cradle. The screw heads should protrude about a quarter of an inch from the cradle.

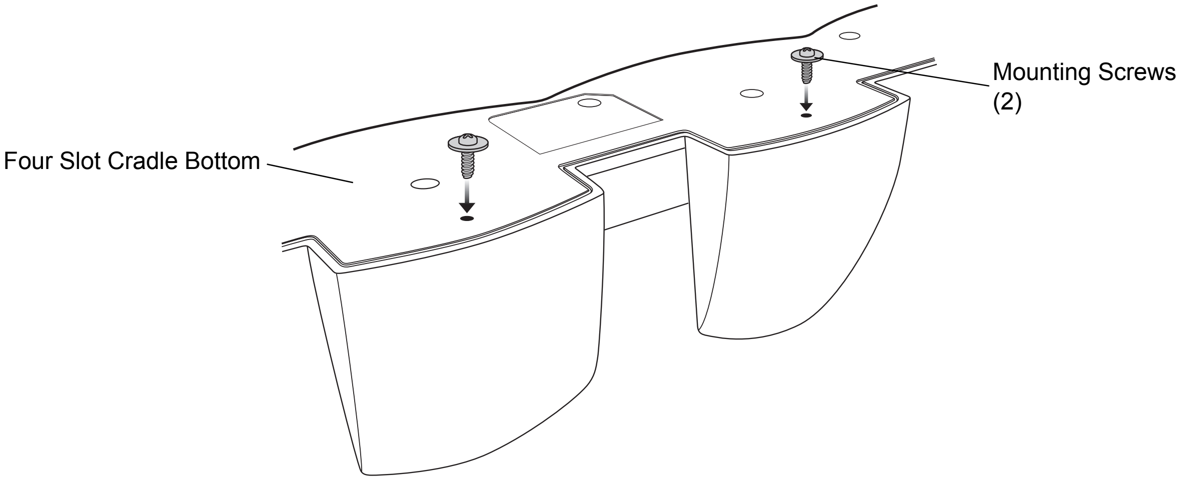


Figure 2-13 *Cradle Mounting Screws*

2. Align the Wall Mount Bracket mounting tabs with the mounting slots in the back of the four slot cradle. Slip the two mounting tabs into mounting slots.

3. Swing the four slot cradle down onto the mounting bracket and align the mounting screws so that they fit into the screw slots.

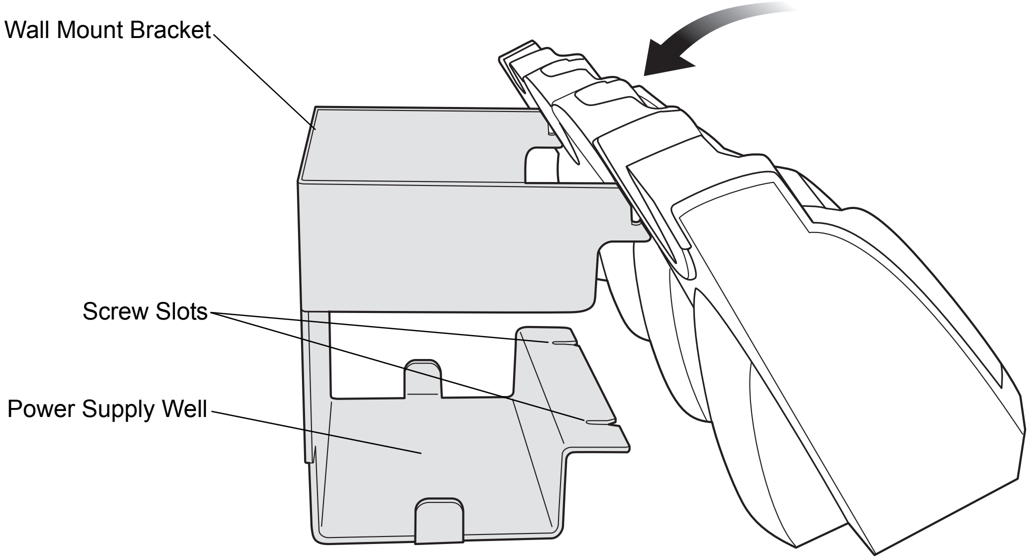


Figure 2-14 *Wall Mount Bracket*

4. Tighten the mounting screws to secure the four slot cradle to the Wall Mount Bracket.

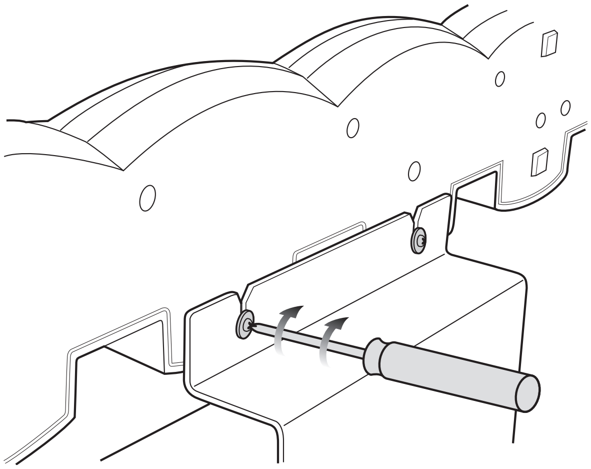


Figure 2-15 *Mounting Screws*

5. Connect the power (see *Figure 2-3 on page 2-6*). The power supply should be located in the power supply well.

Four Slot Spare Battery Charger

CAUTION Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 8-1*.

The Four Slot Spare Battery Charger simultaneously charges up to four spare batteries.

CAUTION Use only a Zebra 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. See the MC3000 User Guide for the power supply regulatory compliance statement.

Setup

Connect the Four Slot Spare Battery Charger to a Zebra approved power source.

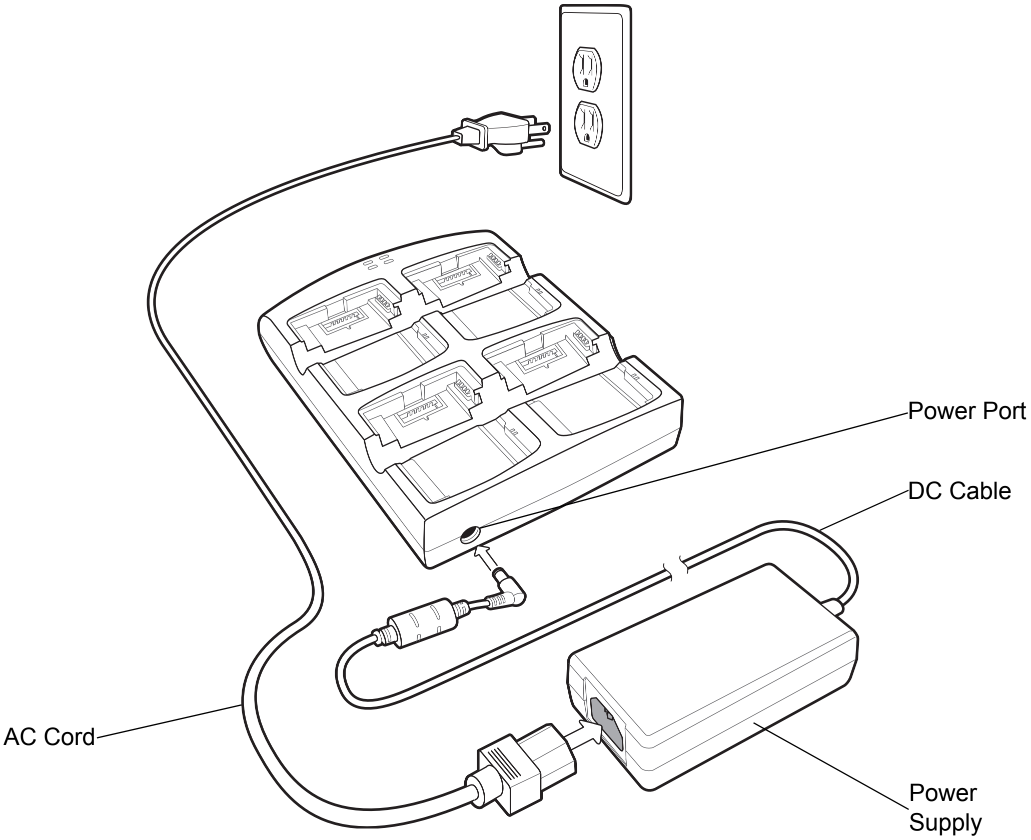


Figure 2-16 *Four Slot Spare Battery Charger Setup*

Spare Battery Charging

To charge up to four MC3000 spare batteries:

1. Insert the spare battery into the spare battery charging slot, bottom first.
2. Pivot the top of the battery down onto the contact pins.

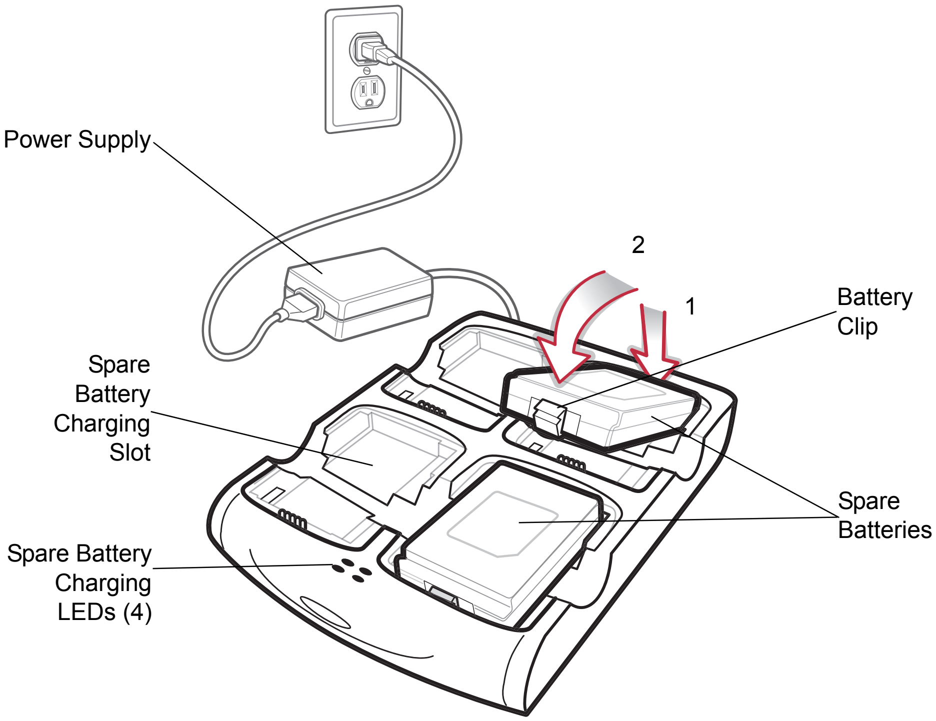


Figure 2-17 *Four Slot Spare Battery Charger*

3. Gently press down on the battery to ensure proper contact. The Standard Battery usually charges in less than four hours and the Extended Life Battery usually charges in less than six hours. See *Table 2-1 on page 2-5* for charging status indications.
4. When charging is complete, press the battery clip and lift battery out of the slot.

LED Charge Indications

The Spare Battery Charging LEDs indicate the spare battery charging status. The Spare Battery Charging LEDs are arranged in the same pattern as the spare battery charging slots so that the charging status of each battery can be identified. See *Table 2-1 on page 2-5* for charging status indications.

Cables

This section describes how to setup and use the cables. The cables are available with a variety of connection capabilities.

The following MC3000 Communication/Charge cables are available:

- Serial (RS232) Charge cable (9-pin D female with power input receptacle)
- USB Client Charge cable (standard-A connector and a barrel receptacle for power).

⚠ ***CAUTION*** Use only a Zebra approved power supply output rated 5.4 VDC and minimum 3 A. Use of an alternative power supply will void the product warranty and may cause product damage. See the MC3000 User Guide for the power supply regulatory compliance statement.

The following printer cables are available directly from the printer manufacturer:

- O'Neil printer cable
- Zebra printer cable.
- Monarch printer cable.

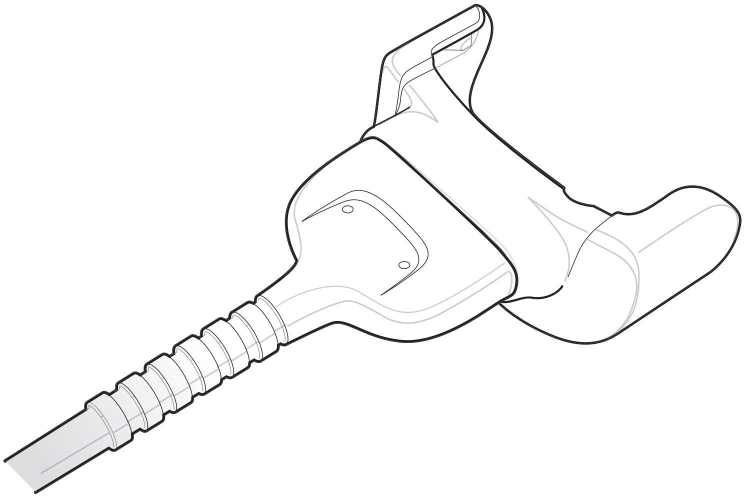


Figure 2-18 *Cables (MC3000 Connector)*

The MC3000 Communication/Charge cables:

- Provide the mobile computer with operating and charging power when used with the Zebra approved power supply.
- Synchronize information between the mobile computer and a host computer. With customized or third party software, it can also synchronize the mobile computer with corporate databases.
- Provide serial connection through the serial pass-through port for communication with a serial device, such as a host computer. For communication setup procedures, see *Serial Communication Setup on page 2-30*.
- Provide USB connection through the USB pass-through port for communication with a USB device, such as a host computer. For communication setup procedures, see *USB Connection Setup on page 2-34*.

Dedicated printer cables, provide communication with a dedicated printer.

Setup

The MC3000 Communication/Charge cables can connect with a serial/USB device, such as a printer or host computer, through its serial or USB port.

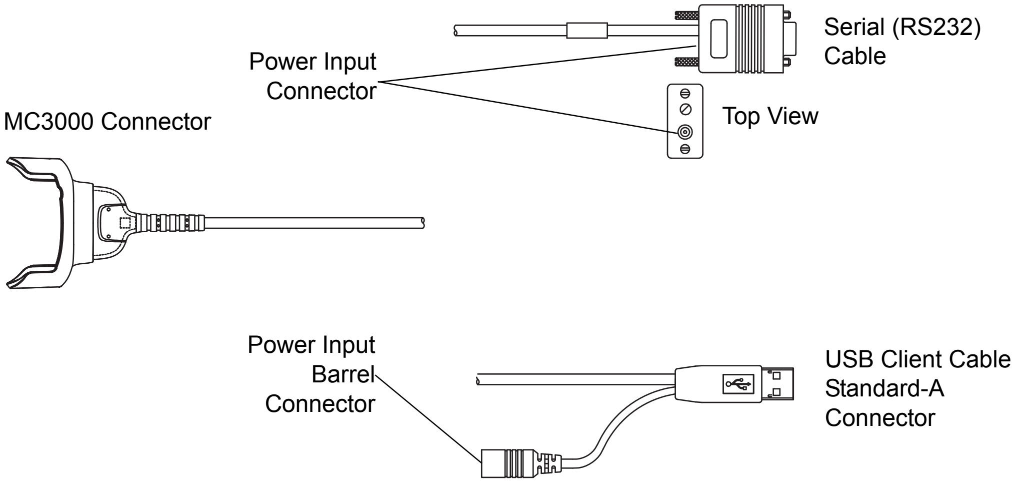


Figure 2-19 *MC3000 Communication/Charge Cables*

Battery Charging

The MC3000 Communication/Charge cables can charge the mobile computer battery and supply operating power.

To charge the mobile computer battery:

1. Connect the MC3000 Communication/Charge cable power input connector to the Zebra approved power source.
2. Attach the bottom of the mobile computer to the MC3000 connector and gently press in until the snaps latch on the mobile computer.
3. The mobile computer amber Charge LED Indicator indicates the mobile computer battery charging status. The Standard Battery usually charges in less than four hours and the Extended Life Battery usually charges in less than six hours. See *Table 2-1 on page 2-5* for charging status indications.
4. When charging is complete, remove the cable by gently pulling the mobile computer and the cable apart until the snaps release the mobile computer.

LED Charge Indications

The MC3000 Communication/Charge cables use the amber Charge LED Indicator to indicate the MC3000 battery charging status. See *Table 2-1 on page 2-5* for charging status indications.

Communication Setup

To connect the MC3000 Communication/Charge cables to a serial or USB device:

1. Connect serial/USB end of the MC3000 Communication/Charge cable into the communications port.
2. Connect the MC3000 connector end to the MC3000 Communication/Charge cable to the mobile computer. For more information on communications setup procedures, see *USB Connection Setup on page 2-34* and/or *Serial Communication Setup on page 2-30*.

Universal Battery Charger (UBC) Adapter

CAUTION Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 8-1*.

The UBC Adapter can be used with a power supply as a standalone spare battery charger or it can be used with the four station UBC2000 to simultaneously charge up to four spare batteries. For additional information on the UBC 2000, refer to the *UBC 2000 Quick Reference Guide, p/n* 70-33188-xx.

CAUTION Use only a Zebra approved power supply output rated 15 VDC and minimum 1.5 A. Use of an alternative power supply will void the product warranty and may cause product damage. See the MC3000 User Guide for the power supply regulatory compliance statement.

Setup

Connect the UBC Adapter to a Zebra approved power source.

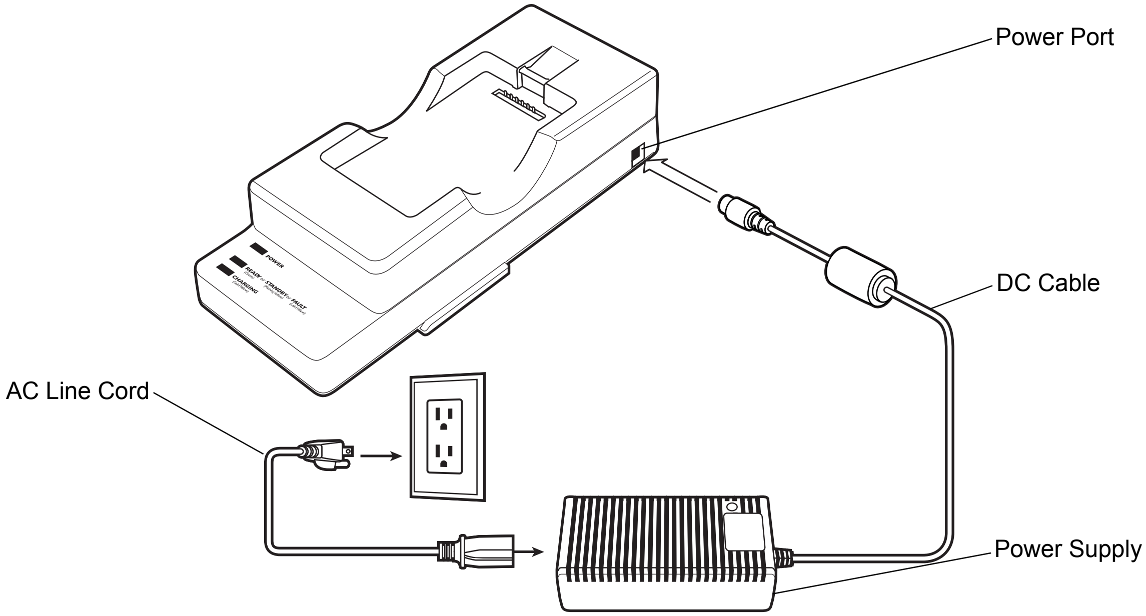


Figure 2-20 *UBC Adapter Setup*

Spare Battery Charging

To charge spare batteries:

1. Insert the spare battery into the spare battery charging slot, bottom first.
2. Pivot the top of the battery down onto the contact pins.

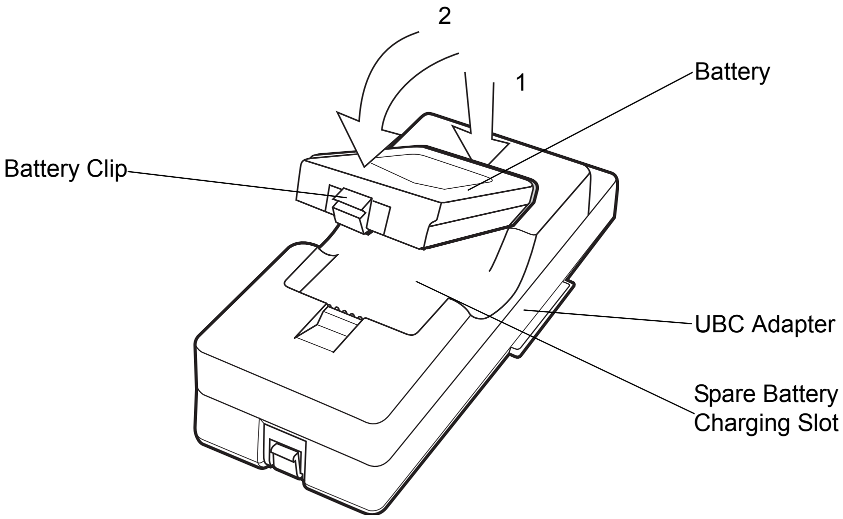


Figure 2-21 *UBC Adapter Battery Insertion*

3. Gently press down on the battery to ensure proper contact. The Standard Battery usually charges in less than four hours and the Extended Life Battery usually charges in less than six hours. See *Table 2-3* for charging status indications.

4. When charging is complete, press the battery clip and lift the battery out of the slot.

UBC Adapter LED Charge Indications

The UBC Adapter charging LEDs indicate the battery charging status.

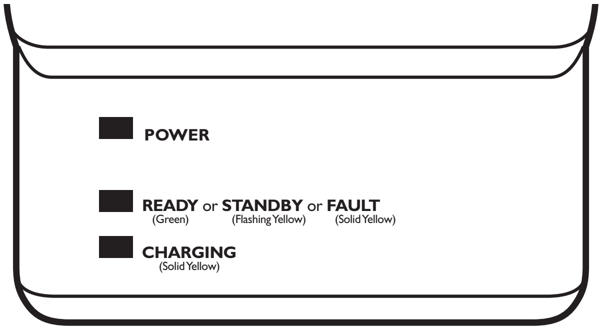


Figure 2-22 *UBC Adapter LEDs*

Table 2-3 *UBC Adapter Charge LED Status Indications*

LED	Indication	Description
POWER	Green	Power is connected to the UBC Adapter.
READY or	Green	Charging complete.

Table 2-3 *UBC Adapter Charge LED Status Indications*

LED	Indication	Description
STANDBY or	Flashing-Yellow	The battery was deeply discharged and is being trickle charged to bring the voltage up to the operating level. After operating level voltage is achieved, the battery charges normally.
FAULT	Yellow	Charging error, check placement of mobile computer/spare battery.
CHARGING	Yellow	Normal charge.

Secure Device Card (Windows CE 5.0 Only)

✓ ***NOTE*** SD Card is not supported on WIndows Mobile 6.1 devices.

The Secure Device (SD) card provides secondary non-volatile storage (the flash memory is slower than RAM). The SD card holder is located under the battery.

⚠ ***CAUTION*** Follow proper Electro-Static Discharge (ESD) precautions to avoid damaging the SD card. Proper ESD precautions include, but are not limited to, working on an ESD mat and ensuring that the operator is properly grounded.

Do not use the SD card slot for any other accessories.

✓ ***NOTE*** Select SD cards with environmental and/or the write cycle performance specifications that meet or exceed the application requirements.

2GB SD Memory Cards are supported on MC3000 with OEM Version 05.26.0000 and higher.

To insert the SD card:

1. Remove the battery (see *Main Battery Removal on page 1-13*).
2. Lift the SD card retaining door.
3. Position the SD card, with the contacts down, into the SD card slot. The SD card corner notch fits into the slot only one way.
4. Snap the retaining door closed.

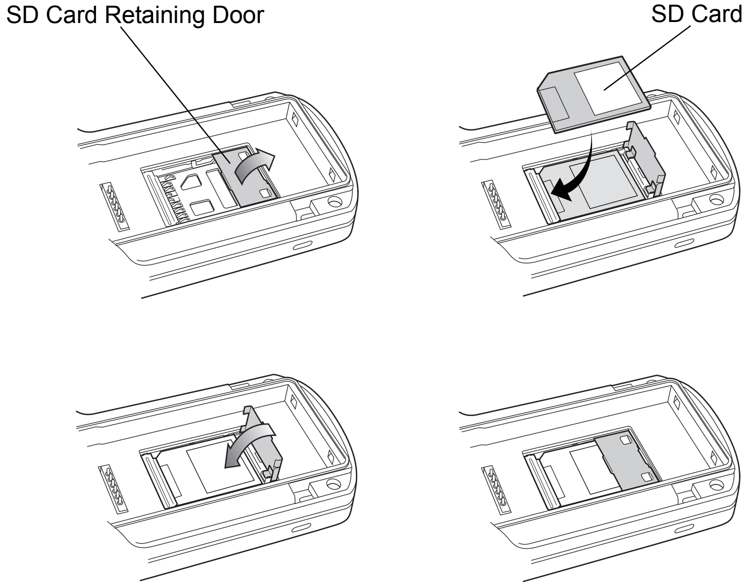


Figure 2-23 *Inserting the SD card*

5. Replace the battery (see *Install Main Battery on page 1-6*).

Copy Files onto the SD Card

The SD card can be used to store files or programs used by the mobile computer. Files may be copied using an available file browser, or using ActiveSync. InkWiz is a provided tool that is being used as an example of how to access data on the SD card.

1. From the **Series 3000 Demo** window, double-tap the **Files** icon. The **InkWiz Example** window appears.

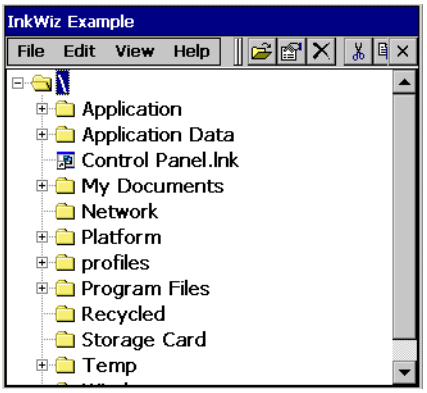


Figure 2-24 *InkWiz Window*

2. To copy a file to the SD card, select a file and tap the file to highlight. The *MSIMGSIZ.DAT* file in the **Temp** partition is being used as an example.
3. Tap **Edit** > **Copy** to copy the file.

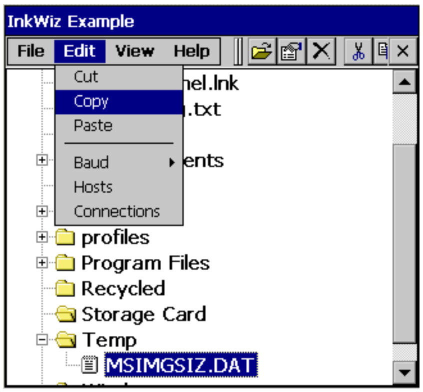


Figure 2-25 *InkWiz, Copy File*

4. Tap the **Storage Card** partition to highlight.
5. Tap the **Edit** > **Paste** to paste the file into the **Storage Card** partition. The **Storage Card** partition now shows that the *MSIMGSIZ.DAT* file is in the **Storage Card** partition.

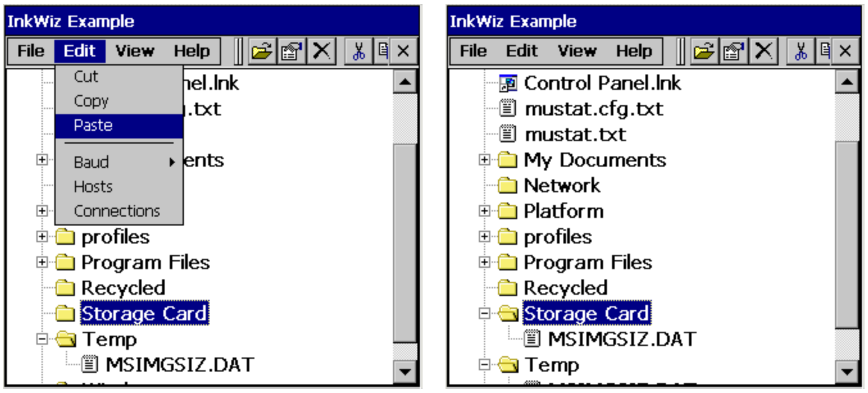
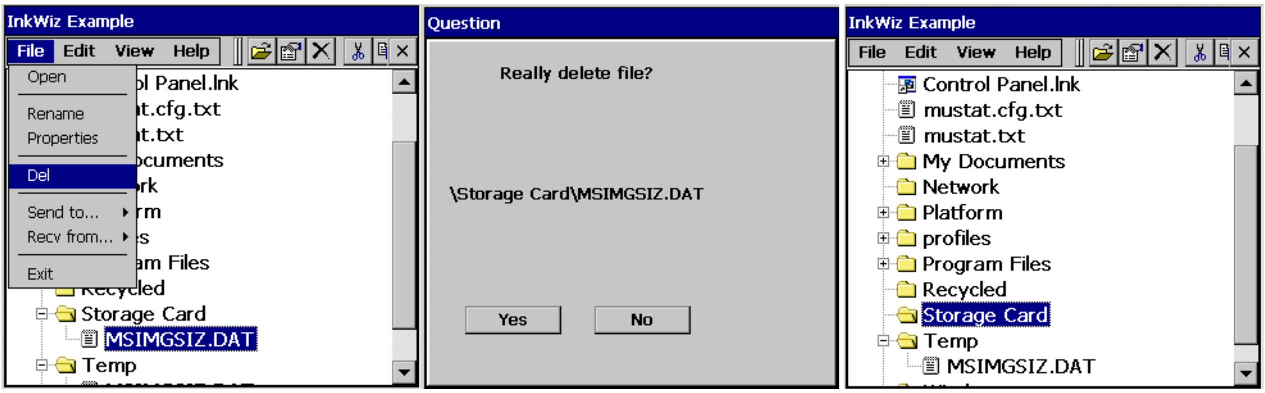


Figure 2-26 *InkWiz, Paste File*

Delete a File From The SD Card

InkWiz is a provided tool that can be used to delete data from the SD card.

1. Tap the *MSIMGSIZ.DAT* file to highlight.
2. Tap **File** > **Del** to delete the file from the Storage Card partition. The **Question** window appears.
3. Tap **Yes** to confirm the file deletion.
4. The **Storage Card** partition now shows that the *MSIMGSIZ.DAT* file is not in the *Storage Card* partition.



Really delete file?

\Storage Card\MSIMGSIZ.DAT

Figure 2-27 *InkWiz, Delete File*

Format an SD Card

Use the **Storage Manager** to format the SD card.

1. Tap **Start** > **Settings** > **Control Panel** to access the **Windows Control Panel**.

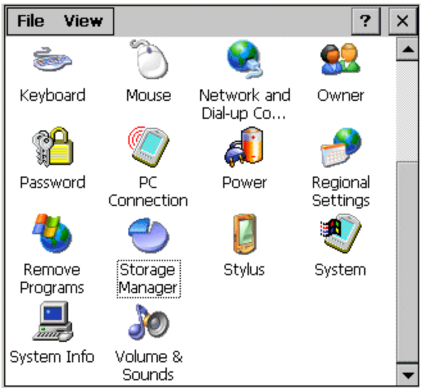
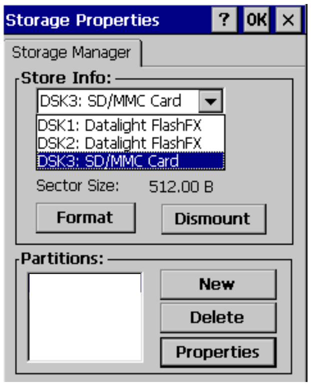


Figure 2-28 *Windows Control Panel*

2. Double tap the **Storage Manager** icon to access the **Storage Properties** Window.

> **CAUTION** Do not select any other partitions for formatting. The DSK3: SD/MMC Card selection is the only entry that can be formatted. Formatting the other partitions may render the mobile computer unusable.



Store Info: DSK3: SD/MMC Card

DSK1: Datalight FlashFX
DSK2: Datalight FlashFX
DSK3: SD/MMC Card

Sector Size: 512.00 B

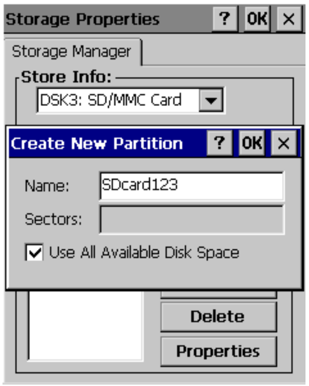
Partitions:

Figure 2-29 *Storage Properties SD Card Select Window*

3. Tap the **Store Info**: drop down menu and select the **DSK3: SD/MMC Card**.

4. Tap **Dismount** to dismount the SD card.

5. If the SD card does not have an existing partition, tap **New**. The **Create New Partition** dialog box appears. If a partition exists, proceed to step 7.



Store Info: DSK3: SD/MMC Card

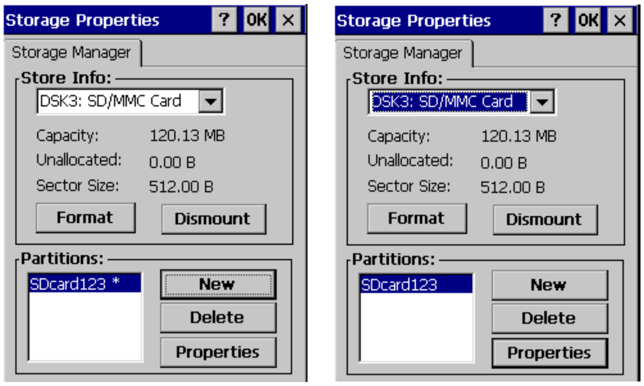
Name: SDcard123

Sectors:

☑ Use All Available Disk Space

Figure 2-30 *Create New Partition Window*

6. In the **Name:** text box enter a partition name, and tap **OK**. The **Storage Properties** window appears.



Store Info: DSK3: SD/MMC Card

Capacity: 120.13 MB

Unallocated: 0.00 B

Sector Size: 512.00 B

Partitions: SDcard123 *

Store Info: DSK3: SD/MMC Card

Capacity: 120.13 MB

Unallocated: 0.00 B

Sector Size: 512.00 B

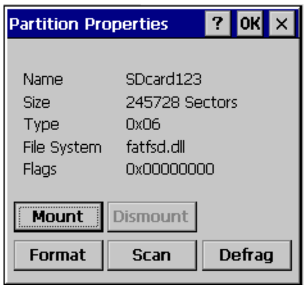
Partitions: SDcard123

Figure 2-31 *Storage Properties Window*

7. The **Storage Properties** window displays the new partition name in the **Partitions:** box. The asterisk next to the partition name, indicates that the partition is mounted. The partition must be dismounted before it can be formatted.

8. Tap **Dismount**, the asterisk next to the partition name disappears indicating that the partition is dismounted.

9. Tap **Properties**, the **Partition Properties** window appears.



Name SDcard123

Size 245728 Sectors

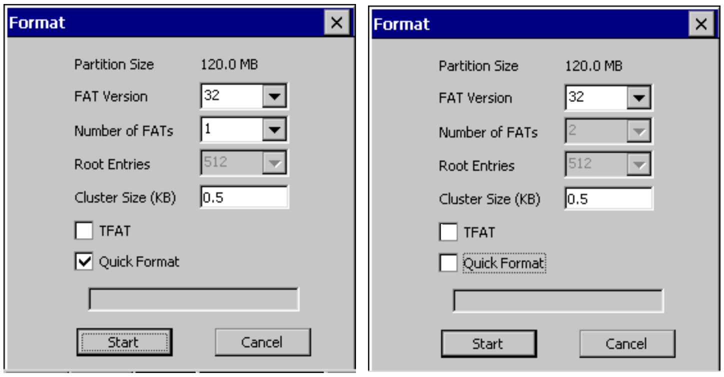
Type 0x06

File System fatfsd.dll

Flags 0x00000000

Figure 2-32 *Partition Properties*

10. Tap **Format**, the **Format** window appears.



Partition Size 120.0 MB

FAT Version 32

Number of FATs 1

Root Entries 512

Cluster Size (KB) 0.5

□ TFAT

☑ Quick Format

Partition Size 120.0 MB

FAT Version 32

Number of FATs 2

Root Entries 512

Cluster Size (KB) 0.5

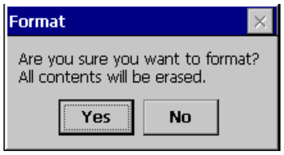
□ TFAT

□ Quick Format

Figure 2-33 *Format Windows*

11. The default settings for the **Format** window are to perform a *Quick Format.* To perform a full format tap the **Quick Format** check box to uncheck.

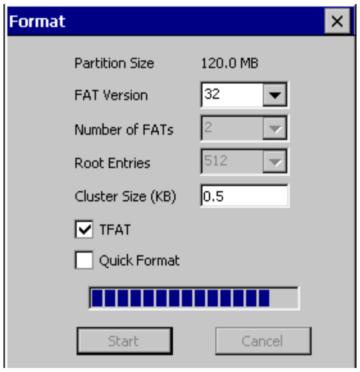
12. Tap **Start**, the **Format** confirmation window appears.



Are you sure you want to format?
All contents will be erased.

Figure 2-34 *Format Confirmation Window*

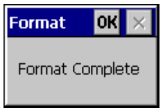
13. Tap **Yes**, the **Format** in progress window appears.



Partition Size 120.0 MB
FAT Version 32
Number of FATs 2
Root Entries 512
Cluster Size (KB) 0.5
☑ TFAT
□ Quick Format

Figure 2-35 *Format In Progress Window*

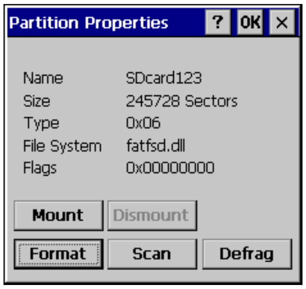
14. The **Format** in progress window completion bar indicates the status of the format. When the format is complete the **Format** complete window appears with a **Format Complete** message.



Format Complete

Figure 2-36 *Format Complete Window*

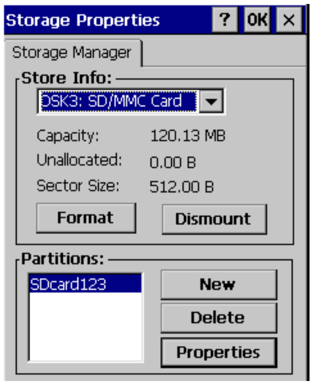
15. Tap **OK**, the **Partition Properties** window appears.



Name SDcard123
Size 245728 Sectors
Type 0x06
File System fatfsd.dll
Flags 0x00000000

Figure 2-37 *Partition Properties and Format Windows*

16. Tap **OK**, the **Storage Properties** window appears.



Storage Properties

Storage Manager

Store Info: DSK3: SD/MMC Card

Capacity: 120.13 MB

Unallocated: 0.00 B

Sector Size: 512.00 B

Partitions: SDcard123

Figure 2-38 *Storage Properties Window*

17. Tap **OK**, to exit the **Storage Manager**.

Serial/USB Communication

This section provides information on installing the appropriate serial/USB communication software and setting up the appropriate accessory to enable serial/USB communication between the mobile computer and the host device.

The mobile computer is capable of communicating with a number of hosts, including development computers, serial devices, printers, etc. The communication accessories serve as data communication devices, enabling the information on the mobile computer to be synchronized with the information on the host device using ActiveSync. With the appropriate accessory and software, the mobile computer can establish a serial connection or a USB connection.

For a serial or USB connection, use one of the following:

- Single Slot Serial/USB cradle
- MC3000 Communication/Charge cables.

Installing Serial/USB Communication Software

To successfully communicate with various host devices communication software, such as Microsoft ActiveSync (version 3.7 or higher) must be installed on the host computer. See *Chapter 3, ActiveSync* for ActiveSync installation procedures.

Communication Setup

The communication setup procedures for the Single Slot Serial/USB cradle and the MC3000 Communication/Charge cables are provided in this section as an example. The serial communication setup procedures are provided in, *Serial Communication Setup on page 2-30* and the USB setup procedures are provided in, *USB Connection Setup on page 2-34*.

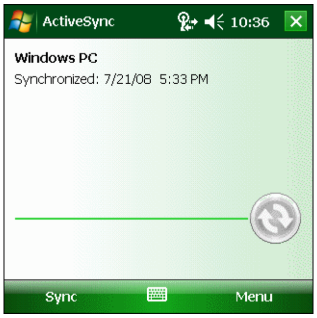
Serial Communication Setup

The serial communication setup is used to set up to communicate between the host and the mobile computer using either a Single Slot Serial/USB cradle or using one of the serial MC3000 Communication/Charge cables.

✓ ***NOTE*** For serial communication using the Single Slot Serial/USB cradle, connect only the serial cable, do not connect both the serial cable and the USB cable. If both serial and USB communication cables are required, the host computer USB port must be disabled in ActiveSync before serial communication can be enabled.

Setting Up a Connection on the Mobile Computer (Windows Mobile 6.1)

1. On the mobile computer tap **Start** > **Programs** > **ActiveSync** to display the **ActiveSync** window.

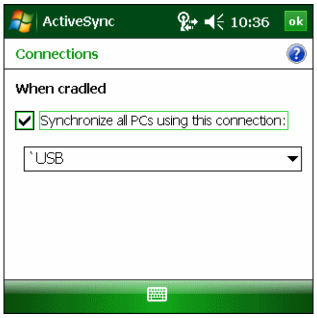


Windows PC

Synchronized: 7/21/08 5:33 PM

Figure 2-39 *ActiveSync Window*

2. Tap **Menu** > **Connections**. The **Connections** window appears.



Connections

When cradled

☑ Synchronize all PCs using this connection:

`USB

Figure 2-40 *Connections Window*

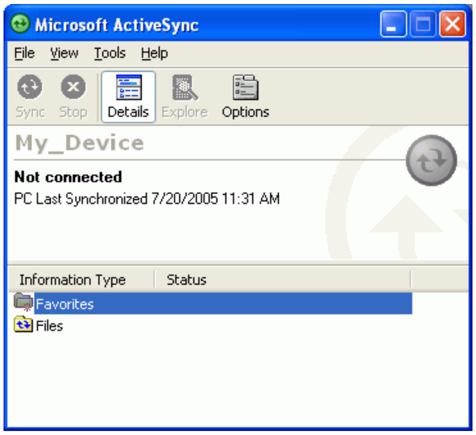
3. Select the *Synchronize all PCs using this connection:* check box.

4. Select the connection (e.g., serial COM port, Bluetooth, or USB) for synchronization from the drop-down list. The default connection for synchronization is USB.

5. Tap **ok** to exit the **Connections** *w*indow.

6. Ensure that ActiveSync is installed on the host computer and a partnership was created.

7. Select **Start** > **Programs** > **Microsoft ActiveSync** on the host computer, if it is not already running. The **Microsoft ActiveSync** window appears.



My_Device

Not connected

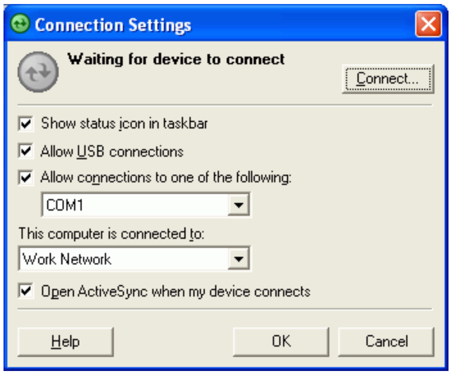
PC Last Synchronized 7/20/2005 11:31 AM

Information Type	Status
Favorites	
Files	

Figure 2-41 *ActiveSync - Not Connected*

✓ ***NOTE*** Every mobile computer should have a unique device name. Never try to synchronize more than one mobile computer to the same name.

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



Connection Settings

Waiting for device to connect

☑ Show status icon in taskbar

☑ Allow USB connections

☑ Allow connections to one of the following:

COM1

This computer is connected to:

Work Network

☑ Open ActiveSync when my device connects

Figure 2-42 *Connection Settings Window*

9. In the **Connection Settings** window, select the appropriate check box for the type of connection being used. If using a serial connection, select the COM port from the drop-down list.

✓ ***NOTE*** If serial, USB and Ethernet communication connections are used, all check boxes can be selected to avoid having to update this window for different connections.

10. Tap **OK** to save any changes made.

11. Ensure the accessory being used to communicate is connected to the host computer and the appropriate power source.

✓ ***NOTE*** The accessory requires a dedicated port. It cannot share a port with any other device. Refer to the host computer user manual supplied to locate the USB ports.

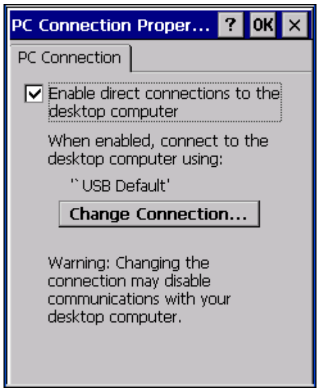
12. Connect the mobile computer to the accessory being used for communication.

13. Power on the mobile computer.

14. If a partnership was already created between the host computer and mobile computer, synchronization occurs automatically upon connection.

Setting Up a Serial Connection on the Mobile Computer (Windows CE 5.0)

1. On the mobile computer, tap **> Settings > Control Panel > PC Connection icon.** The **PC Connection Properties** window appears.



☑ Enable direct connections to the desktop computer

When enabled, connect to the desktop computer using:

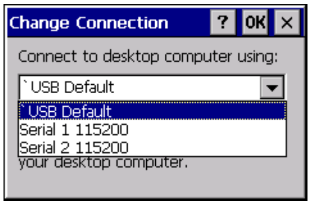
'`USB Default'

Warning: Changing the connection may disable communications with your desktop computer.

Figure 2-43 *PC Connection Properties Window*

2. Tap the **Change Connection** button.

3. Select the connection type from the drop-down list.



Connect to desktop computer using:

`USB Default

`USB Default
Serial 1 115200
Serial 2 115200

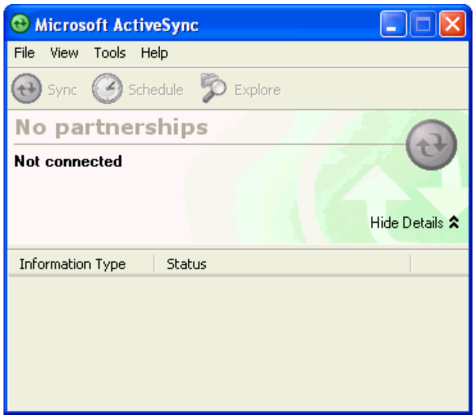
your desktop computer.

Figure 2-44 *Change Connection Window*

4. Tap **OK** to exit the **Change Connection** window and tap **OK** to exit the **PC Connection Properties** window.

5. Ensure that ActiveSync was installed on the host computer and a partnership was created. See *Setting Up an ActiveSync Connection on the Host Computer on page 3-3* for more information.

6. If *ActiveSync* is not running on the host computer, select **Start** > **Programs** > **Microsoft ActiveSync** to start **ActiveSync**, to start.



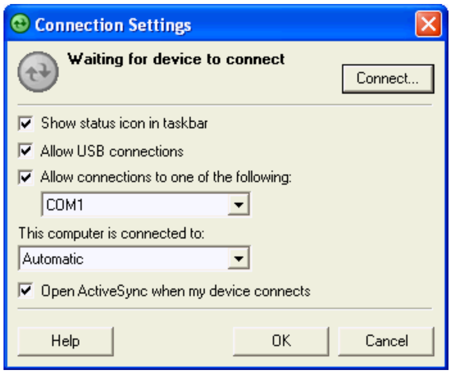
No partnerships

Not connected

Figure 2-45 *ActiveSync - Not Connected*

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

8. Select the appropriate COM port for the host computer.



Connection Settings

Waiting for device to connect

☑ Show status icon in taskbar

☑ Allow USB connections

☑ Allow connections to one of the following:

COM1

This computer is connected to:

Automatic

☑ Open ActiveSync when my device connects

Figure 2-46 *Serial Connection Setting*

9. Tap **OK** to save any changes made.

> ✓ ***NOTE*** Every mobile computer should have a unique device name. Never try to synchronize more than one mobile computer to the same name.

10. Connect the device to the host computer. See *Figure 2-1 on page 2-3* to set up a Single Slot Serial/USB cradle, or see *Figure 2-19 on page 2-19* for cable connections.

> ✓ ***NOTE*** The cradle requires a dedicated port. It cannot share a port with an internal modem or other device. Refer to the host computer documentation to locate the serial port(s).

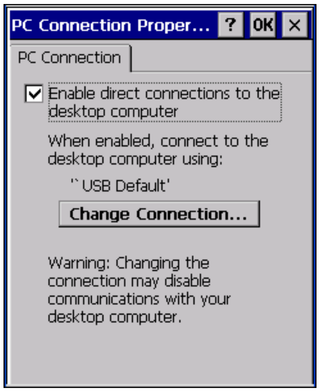
11. Upon connection, synchronization occurs automatically.

USB Connection Setup

The USB communication setup is used to set up to communicate between the host and the mobile computer using either a Single Slot Serial/USB cradle or using one of the serial MC3000 Communication/Charge cables.

> ✓ ***NOTE*** For serial communication using the Single Slot Serial/USB cradle, connect only the USB cable, do not connect both the USB cable and the serial cable. If both serial and USB communication cables are required, the host computer USB port is the default setting in ActiveSync.

1. On the mobile computer, tap **> Settings > Control Panel > PC Connection icon.** The **PC Connection Properties** window appears.



☑ Enable direct connections to the desktop computer

When enabled, connect to the desktop computer using:

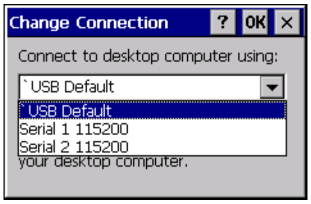
'`USB Default'

Warning: Changing the connection may disable communications with your desktop computer.

Figure 2-47 *PC Connection Properties Window*

2. Tap the **Change Connection** button.

3. Select the connection type from the drop-down list.



Connect to desktop computer using:

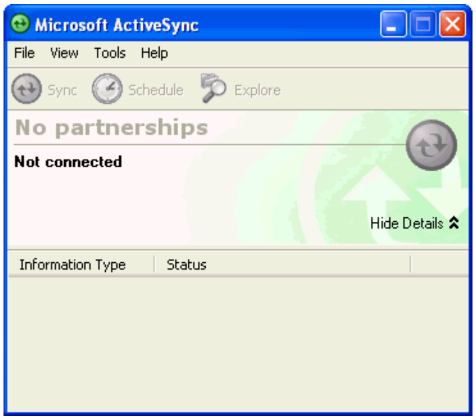
USB Default

USB Default
Serial 1 115200
Serial 2 115200

your desktop computer.

Figure 2-48 *Change Connection Window*

4. Tap **OK** to exit the **Change Connection** window and tap **OK** to exit the **PC Connection Properties** window.
5. Ensure that ActiveSync was installed on the host computer and a partnership was created. See *Setting Up an ActiveSync Connection on the Host Computer on page 3-3* for more information.
6. If **ActiveSync** is not running on the host computer, select **Start** > **Programs** > **Microsoft ActiveSync** to start ActiveSync, to start
7. Start ActiveSync, if it is not running on the host computer. To start, select **Start** > **Programs** > **Microsoft ActiveSync**.



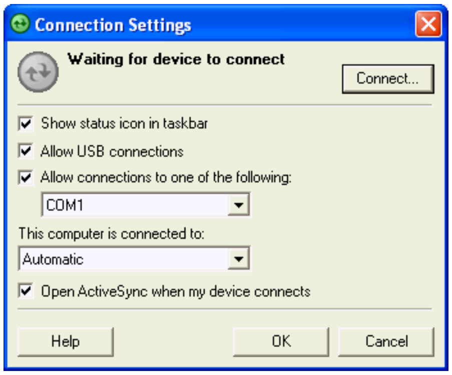
No partnerships

Not connected

Information Type	Status

Figure 2-49 *ActiveSync - Not Connected*

8. In the **ActiveSync** window, select **File** > **Connection Settings**, the **Connection Settings** window appears.
9. Confirm that the **Allow USB connections** check box is selected.



Waiting for device to connect

☑ Show status icon in taskbar

☑ Allow USB connections

☑ Allow connections to one of the following:

COM1

This computer is connected to:

Automatic

☑ Open ActiveSync when my device connects

Figure 2-50 *USB Connection Setting*

10. Tap **OK** to save any changes made.

✓ ***NOTE*** Every mobile computer should have a unique device name. Never try to synchronize more than one mobile computer to the same name.

11. Connect the device to the host computer. See *Figure 2-1 on page 2-3* to set up a Single Slot Serial/USB cradle, or see *Figure 2-19 on page 2-19* for cable connections.

✓ ***NOTE*** The cradle requires a dedicated port. It cannot share a USB port with any other device. Refer to the computer user manual supplied to locate the USB(s).

12. Upon connection, synchronization occurs automatically.

Cradle/Cable Setup

To use ActiveSync with a cradle or a MC3000 Communication/Charge cable, see *Setting Up a Serial Connection on the Mobile Computer (Windows CE 5.0) on page 2-32* and *USB Connection Setup on page 2-34* for communication setup procedures.

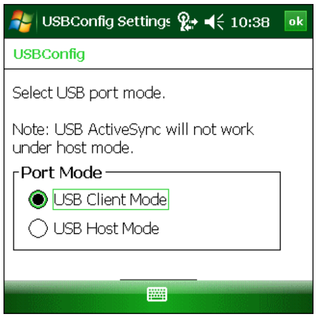
USB Host Communication Setup

NOTE USB Host mode is only available on Windows Mobile 6.1 devices.

The mobile computer can be configured as a USB host device for use with USB client devices.

To configure the mobile computer as a USB host:

1. Tap **Start** > **Settings** > **System** > **USBConfig** icon.



Select USB port mode.

Note: USB ActiveSync will not work under host mode.

Port Mode

● USB Client Mode

○ USB Host Mode

Figure 2-51 *USBConfig Settings Window*

2. Tap the **USB Host Mode** radio button.
3. Tap **OK**.

NOTE When the mobile computer is configured a a USB host, it cannot ActiveSync with a host computer.

To configure the mobile computer as a USB client:

1. Tap **Start** > **Settings** > **System** > **USBConfig** icon.
2. Tap the **USB Client Mode** radio button.
3. Tap **OK**.
4. Remove the mobile computer from the cradle or CAM.
5. Re-insert the mobile computer into a cradle or re-connect the CAM.

Chapter 3 ActiveSync

Introduction

To communicate with various host devices, install Microsoft ActiveSync (version 4.5 or higher) on the host computer. Use ActiveSync to synchronize information on the mobile computer with information on the host computer. Changes made on the mobile computer or host computer appear in both places after synchronization.

✓ ***NOTE*** When a mobile computer with Windows Mobile 6.1 is connected to a host computer and an ActiveSync connection is made, the WLAN and WWAN radios (if applicable) are disabled. This is a Microsoft security feature to prevent connection to two networks at the same time.

ActiveSync software:

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

Installing ActiveSync

To install ActiveSync on the host computer, download version 4.5 or higher from the Microsoft web site at http://www.microsoft.com. Refer to the installation included with the ActiveSync software.

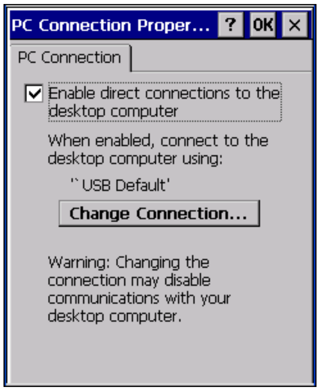
Mobile Computer Setup

✓ ***NOTE*** Microsoft recommends installing ActiveSync on the host computer before connecting the mobile computer.

The mobile computer can be set up to communicate either with a serial connection or a USB connection. Chapter 2, Accessories provides the accessory setup and cable connection information for use with the mobile computer. The mobile computer communication settings must be set to match the communication settings used with ActiveSync.

On Windows CE 5.0 Devices:

1. On the mobile computer tap **Start** > **Settings** > **Control Panel** > **PC Connection** icon. The **PC Connection Properties** window appears.



☑ Enable direct connections to the desktop computer

When enabled, connect to the desktop computer using:

'`USB Default'

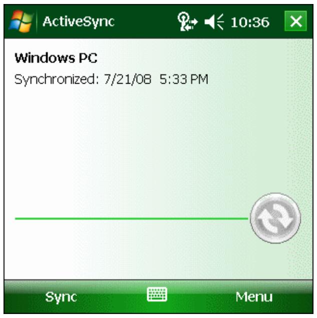
Warning: Changing the connection may disable communications with your desktop computer.

Figure 3-1 *PC Connection Properties Window*

2. Tap the **Change Connection** button.
3. Select the connection type from the drop-down list.
4. Tap **OK** to exit the **Change Connection** window and tap **OK** to exit the **PC Connection Properties** window.
5. Proceed with installing ActiveSync on the host computer and setting up a partnership.

On Windows Mobile 6.1 Devices:

1. On the mobile computer tap **Start** > **Programs** > **ActiveSync** icon. The **ActiveSync** window appears.



Windows PC

Synchronized: 7/21/08 5:33 PM

Figure 3-2 *ActiveSync Window*

2. Tap **Menu** > **Connections**.

3. Select the connection type from the drop-down list.
4. Tap **OK** to exit the **Connections** window and tap **OK** to exit the **ActiveSync** window.
5. Proceed with installing ActiveSync on the host computer and setting up a partnership.

Setting Up an ActiveSync Connection on the Host Computer

To start ActiveSync:

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

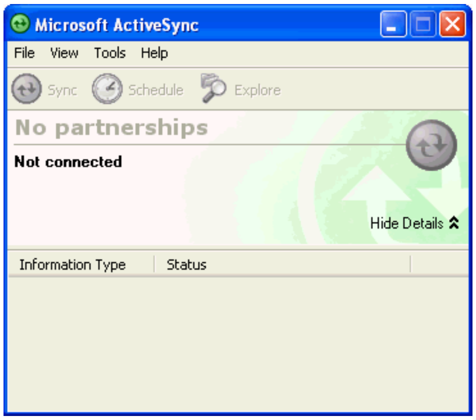
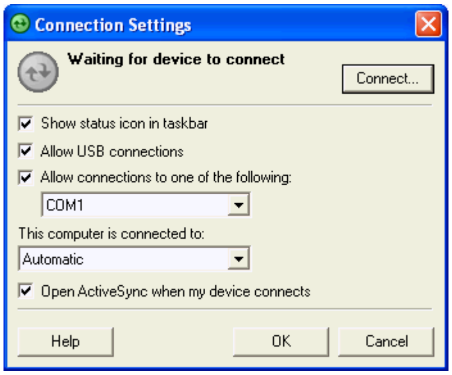


Figure 3-3 *ActiveSync Window*

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

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



Waiting for device to connect

☑ Show status icon in taskbar

☑ Allow USB connections

☑ Allow connections to one of the following:

COM1

This computer is connected to:

Automatic

☑ Open ActiveSync when my device connects

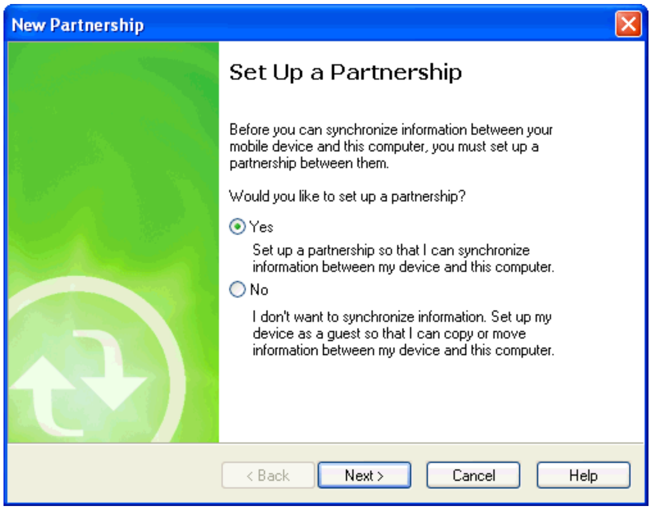
Figure 3-4 *Connection Settings Window*

3. Select the appropriate check box for the type of connection used.
4. Select the **Show status icon in Taskbar** check box.
5. Select **OK** to save any changes made.

Setting up a Partnership with a Windows CE 5.0 Device

To set up a partnership with a Windows CE 5.0 device:

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



New Partnership

Set Up a Partnership

Before you can synchronize information between your mobile device and this computer, you must set up a partnership between them.

Would you like to set up a partnership?

● Yes

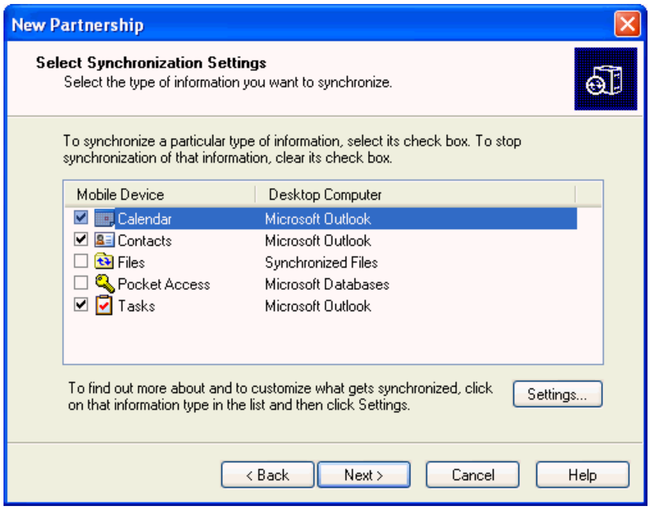
Set up a partnership so that I can synchronize information between my device and this computer.

○ No

I don't want to synchronize information. Set up my device as a guest so that I can copy or move information between my device and this computer.

Figure 3-5 *New Partnership Window*

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



New Partnership

Select Synchronization Settings

Select the type of information you want to synchronize.

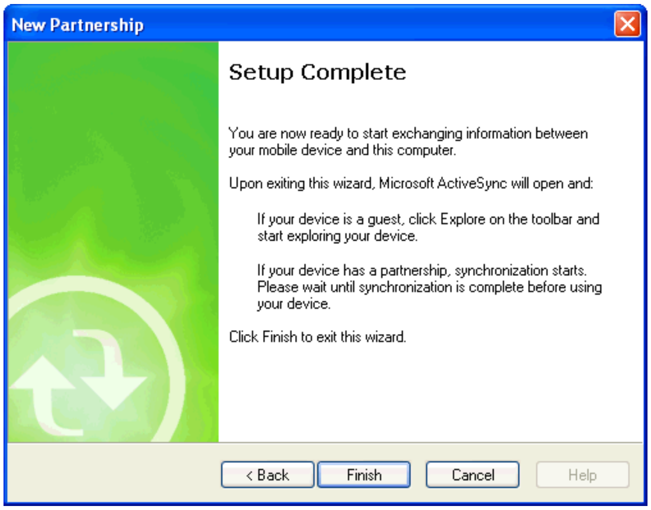
To synchronize a particular type of information, select its check box. To stop synchronization of that information, clear its check box.

Mobile Device	Desktop Computer
☑ Calendar	Microsoft Outlook
☑ Contacts	Microsoft Outlook
☐ Files	Synchronized Files
☐ Pocket Access	Microsoft Databases
☑ Tasks	Microsoft Outlook

To find out more about and to customize what gets synchronized, click on that information type in the list and then click Settings.

Figure 3-6 *Select Synchronization Setting Window*

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



Setup Complete

You are now ready to start exchanging information between your mobile device and this computer.

Upon exiting this wizard, Microsoft ActiveSync will open and:

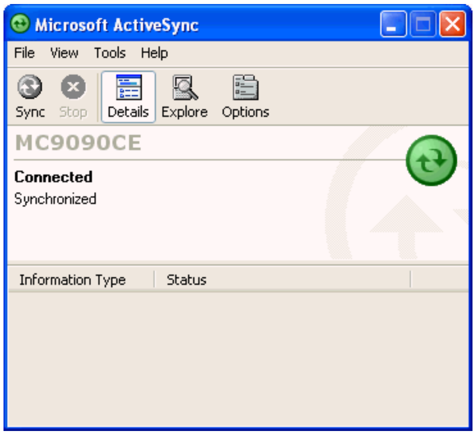
If your device is a guest, click Explore on the toolbar and start exploring your device.

If your device has a partnership, synchronization starts. Please wait until synchronization is complete before using your device.

Click Finish to exit this wizard.

Figure 3-7 *Setup Complete Window*

5. Click **Finish**.



MC9090CE

Connected

Synchronized

Figure 3-8 *ActiveSync Connected Window*

During the first synchronization, information stored on the mobile computer is copied to the host computer. When the copy is complete and all data is synchronized, the mobile computer can be disconnect 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, detailed information is provided in the EMDK Windows CE Help File for Zebra Mobile Computers.

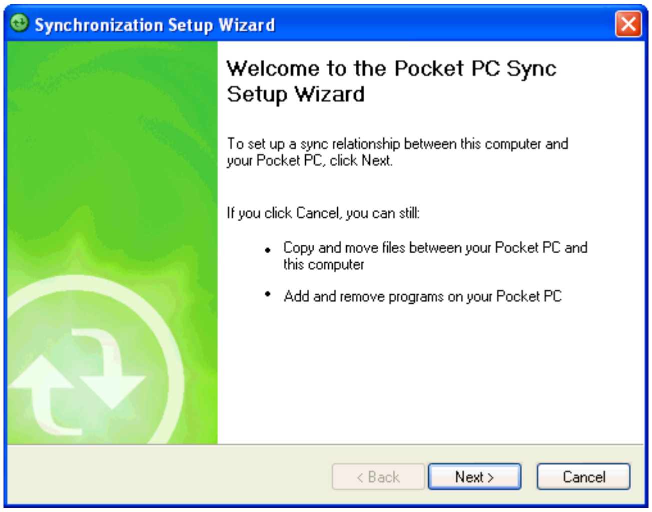
For more information about using ActiveSync, start ActiveSync on the host computer, then see ActiveSync Help.

Synchronization with a Windows Mobile 6.1 Device

✓ ***NOTE*** When a mobile computer with Windows Mobile 6.1 is connected to a host computer and an ActiveSync connection is made, the WLAN and WWAN radios (if applicable) are disabled. This is a Microsoft security feature to prevent connection to two networks at the same time.

To synchronize with a Windows Mobile 6.1 device:

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



Synchronization Setup Wizard

Welcome to the Pocket PC Sync Setup Wizard

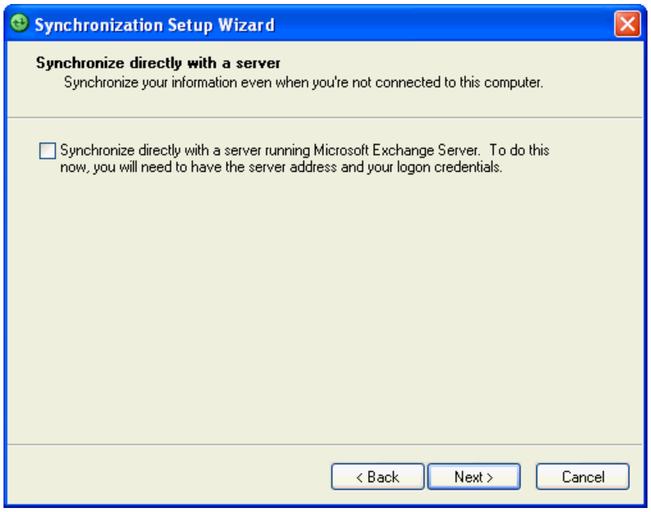
To set up a sync relationship between this computer and your Pocket PC, click Next.

If you click Cancel, you can still:

- Copy and move files between your Pocket PC and this computer
- Add and remove programs on your Pocket PC

Figure 3-9 *Synchronization Setup Wizard Window*

2. Click **Next**.



Synchronization Setup Wizard

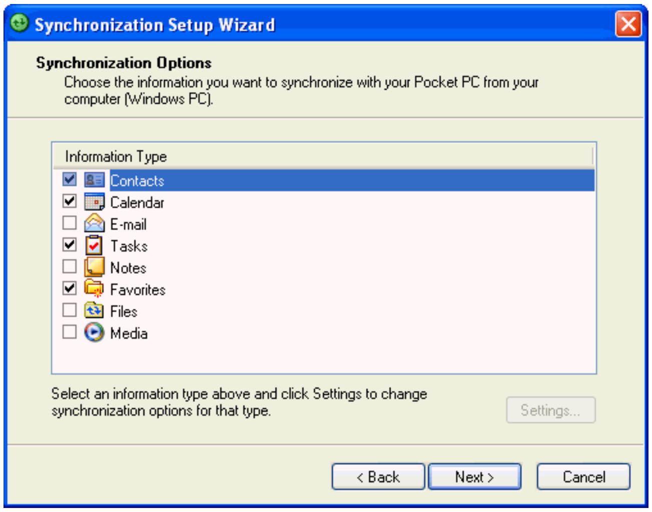
Synchronize directly with a server

Synchronize your information even when you're not connected to this computer.

☐ Synchronize directly with a server running Microsoft Exchange Server. To do this now, you will need to have the server address and your logon credentials.

Figure 3-10 *Synchronization Directly With a Server Window*

3. Select the check box to synchronize with a server running Microsoft Exchange.
4. Click **Next**.



Synchronization Options

Choose the information you want to synchronize with your Pocket PC from your computer (Windows PC).

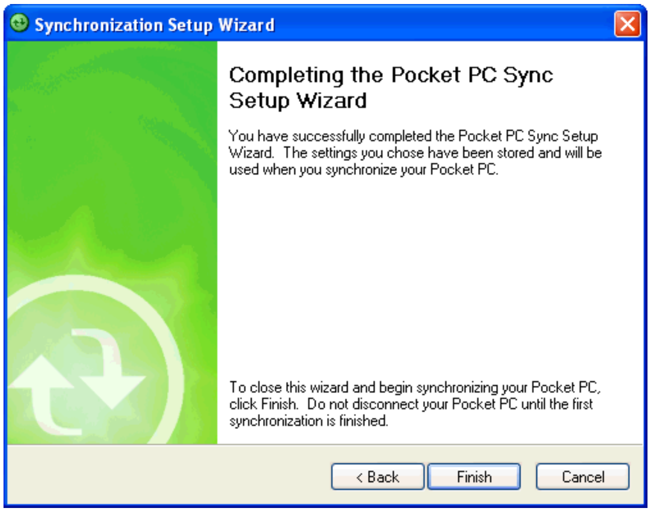
Information Type

- ☑ Contacts
- ☑ Calendar
- □ E-mail
- ☑ Tasks
- □ Notes
- ☑ Favorites
- □ Files
- □ Media

Select an information type above and click Settings to change synchronization options for that type.

Figure 3-11 *Synchronization Option Window*

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



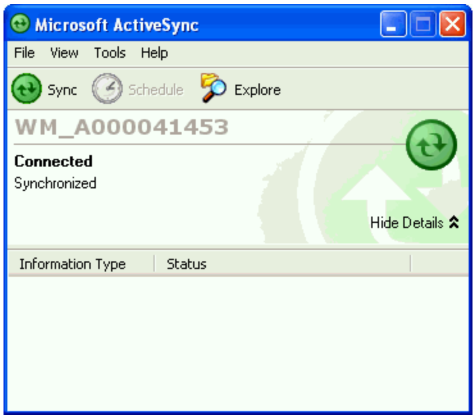
Completing the Pocket PC Sync Setup Wizard

You have successfully completed the Pocket PC Sync Setup Wizard. The settings you chose have been stored and will be used when you synchronize your Pocket PC.

To close this wizard and begin synchronizing your Pocket PC, click Finish. Do not disconnect your Pocket PC until the first synchronization is finished.

Figure 3-12 *Wizard Complete Window*

6. Click **Finish**.



WM_A000041453

Connected

Synchronized

Figure 3-13 *ActiveSync Connected Window*

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

✓ ***NOTE*** The first ActiveSync operation must be performed with a local, direct connection. Windows Mobile retains partnerships information after a cold boot.

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

Chapter 4 Application Deployment for Windows CE 5.0

Software Installation on Development PC

To develop applications to run on the mobile computer, use one or both of the following:

- Enterprise Mobility Developer Kit (EMDK) for C
- Platform Software Developer Kit (Platform SDK) for MC3000
- Device Configuration Package (DCP) for MC3000.

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

The *Windows CE Platform SDK for MC3000c50* is used in conjunction with the EMDK for C to create Windows CE applications for the MC3000 mobile computer. The Platform SDK installs a new Windows CE device type and its associated libraries onto the development PC.

The DCP is required to create and download hex images that represent flash partitions to the mobile computer. The DCP includes documentation, flash partitions, Terminal Configuration Manager (TCM) and the associated TCM scripts.

Required System Configurations

The minimum host system configuration required to use the EMDK for C and DCP for MC3000 is:

- IBM-compatible host computer with Pentium 450 MHz processor or higher
- Microsoft Windows XP or Microsoft Windows 2000 operating system
- 128 MB RAM
- 100 MB available hard disk space
- CD-ROM drive
- One available serial port
- Mouse

- Adobe® Acrobat® Reader® 7.0 or higher, available at the Microsoft web site: http://www.microsoft.com
- Microsoft ActiveSync version 3.7 or higher, available at the Microsoft web site: http://www.microsoft.com
- Microsoft Embedded Visual C++ v4.0 with SP2, available at the Microsoft web site: http://www.microsoft.com

Device Configuration Package

To download and install the DCP:

1. Download the DCP from the Support Central web site: http://www.zebra.com/support.
   a. Select *Mobile Computers*. The *Mobile Computer Products* page displays.
   b. Select *MC3000*. The *MC3000 Product* page displays.
   c. On the *MC3000 Product* page, select the *Device Configuration Package (DCP) for MC3000* from the *Software Downloads* section. The *Device Configuration Package* page displays.
   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 components of the DCP from the *Device Configuration Package (DCP) for MC3000* program group of the Windows Start menu.

Components

Table 4-1 lists the MC3000 DCP components and their locations.

Table 4-1 *DCP for MC3000 Components and Locations*

Component	Description	Directory Location
Files that make up the flash partitions	Used to configure the mobile computer.	\Program Files\Symbol Device Configuration Packages\MC3000\v1.0\Flash Folders
Hex image - default location	Loads onto the mobile computer for configuration.	\Program Files\Symbol Device Configuration Packages\MC3000\v1.0\Hex Images
Documentation	Documents that provide guidance on using and integrating the MC3000.	\Program Files\Symbol Device Configuration Packages\MC3000\v1.0
Readme	Contains important information for the DCP.	\Program Files\Symbol Device Configuration Packages\MC3000\v1.0
Scripts	Used to customize flash partitions.	\Program Files\Symbol Device Configuration Packages\MC3000\v1.0\TCM Scripts
TCM	An application used to customize flash file system partitions for the mobile computer.	\Program Files\Symbol\TCM2
Tools (Keyboard remap, if any)	Used in developing applications for the mobile computer.	\Program Files\Symbol Device Configurations package\MC3000\v1.0\Tools\kbtool
Note: Directory locations may vary depending upon software versions.		

Table 4-1 *DCP for MC3000 Components and Locations (Continued)*

Component	Description	Directory Location
Start Menu: Readme Documentation TCM WEB Updates	Specifies items to appear in the Start menu.	\Documents and Settings\All Users\Start Menu\Programs
Note: Directory locations may vary depending upon software versions.		

Platform SDK

Different Platform SDKs are required for the Microsoft® Windows CE .NET 5.0 Professional and Microsoft® Windows CE .NET 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. Select *Mobile Computers*. The *Mobile Computer Products* page displays.
   b. Select *MC3000*. The *MC3000 Product* page displays.
   c. On the *MC3000 Product* page, select the appropriate *Platform SDK for MC3000* from the *Software Downloads* section. The *Platform SDK* page displays.
   d. Save the .exe file to the development computer.
2. Run the file and follow the screen prompts to install.

EMDK for C

To download and install the EMDK for C:

1. Download the EMDK from the Support Central web site, http://www.zebra.com/support.
   a. Select *Mobile Computers*. The *Mobile Computer Products* page displays.
   b. Select *MC3000*. The *MC3000 Product* page displays.
   c. On the *MC3000 Product* page, select the appropriate *Enterprise Mobility Developer Kit for C* from the *Software Downloads* section. The *Enterprise Mobility Developer Kit for C* page displays.
   d. Select the latest version, and save the .exe file to the development computer.
2. Locate the .exe file on the development computer, double-click the executable file and follow the install screen prompts.
3. Once installed, access the components of the EMDK for C from the *Enterprise Mobility Developer Kit for C* program group of the *Windows Start* menu.
4. The sample applications provide examples of how to interface with the Zebra API functions. To build a sample application, open the Samples folder from the Windows *Start* menu. Open the folder for the desired sample

and then open the project file. The project file has an extension of VCP. Microsoft Visual C++ v4.0 automatically launches. Select *WinCE* as the Active WCE Configuration. Select Win32 (WCE ARMV4) Debug as the active configuration.

✓ ***NOTE*** If both Microsoft Visual C++ v3.0 and Microsoft Visual C++ v4.0 are installed on the development computer, ensure Microsoft Visual C++ v4.0 launches.

Components

The sample applications provide examples of how to interface with the Zebra API functions. To build a sample application, open the Samples folder from the Windows *Start* menu. Open the folder for the desired sample and then open the project file. The project file has an extension of VCP. Microsoft Visual C++ v4.0 automatically launches. Select *WinCE* as the Active WCE Configuration. Select Win32 (WCE ARMV4) Debug as the active configuration.

✓ ***NOTE*** If both Microsoft Visual C++ v3.0 and Microsoft Visual C++ v4.0 are installed on the development computer, ensure Microsoft Visual C++ v4.0 launches.

Table 4-2 lists the EMDK for C components.

Table 4-2 *EMDK for C Components and Locations*

Components	Directory Location
EMDK (API) Help file and Readme file	\Program Files\Symbol Mobility Developer Kit v*x.x* for C\
Sample applications for quick-start development	\Program Files\Symbol Mobility Developer Kit v*x.x* for C\Samples\evc\
Header files with API prototypes and structures*	\Program Files\Windows CE Tools\wce420\WinCE\Include\armv4
Import Library files*	\Program Files\Windows CE Tools\wce420\WinCE\Lib\armv4
Start Menu Readme Help Platform Integrator Samples Web Updates	\Documents and Settings\All Users\Start Menu\Programs
* The header files and library files are time and date stamped so they can be easily identified in the armv4 directories. The “date” is the date on which the software release was assembled and the time is the version of the release. For example, a time of 1:00 signifies version 1.0.	
Note: Directory locations may vary depending upon software versions.	

Installing Other Development Software

Developing applications for the mobile computer may require installing other development software, such as application development environments, on the development PC. Follow the installation instructions provided with the software.

Software Updates

Download updates to the EMDK for C from the Support Central web site at: http://www.zebra.com/support. Check this site periodically for important updates and new software versions.

Deployment

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

Download/software installations can be performed using:

- ActiveSync
- Initial Program Loader (IPL)
- Mobility Services Platform (MSP)
- SD card.

ActiveSync

Use ActiveSync to copy files and/or programs from a host computer to the mobile computer.

Copying Files

1. Ensure that ActiveSync is installed on the host computer and that a partnership was created. For more information see, *Chapter 3, ActiveSync*.
2. Connect the mobile computer to the host computer using a Single Slot Serial/USB cradle or an appropriate cable. See, *Chapter 2, Accessories* for connection information.
3. On the host computer, select **Start** > **Programs** > **ActiveSync**.

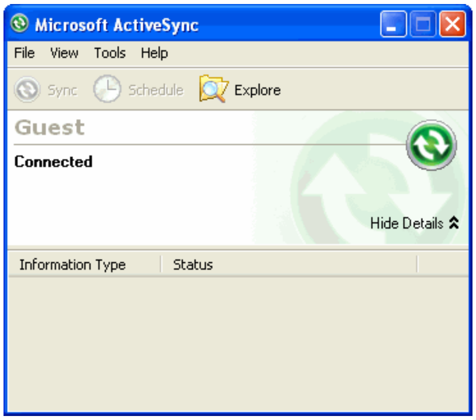
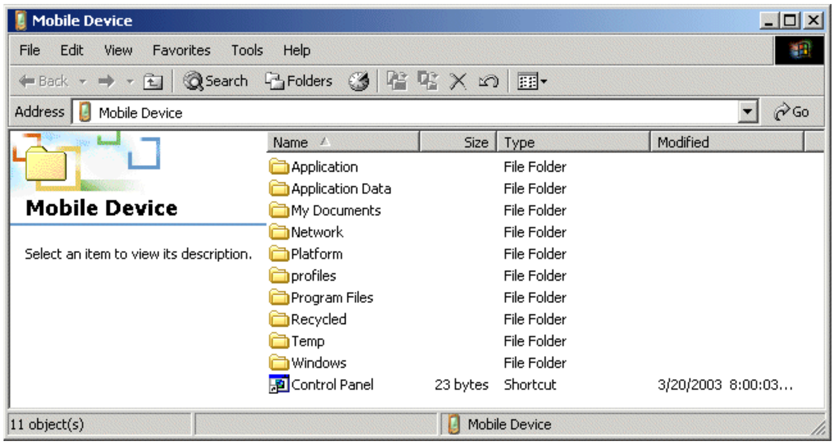


Figure 4-1 *ActiveSync Connected Window*

4. Select *Explore*.

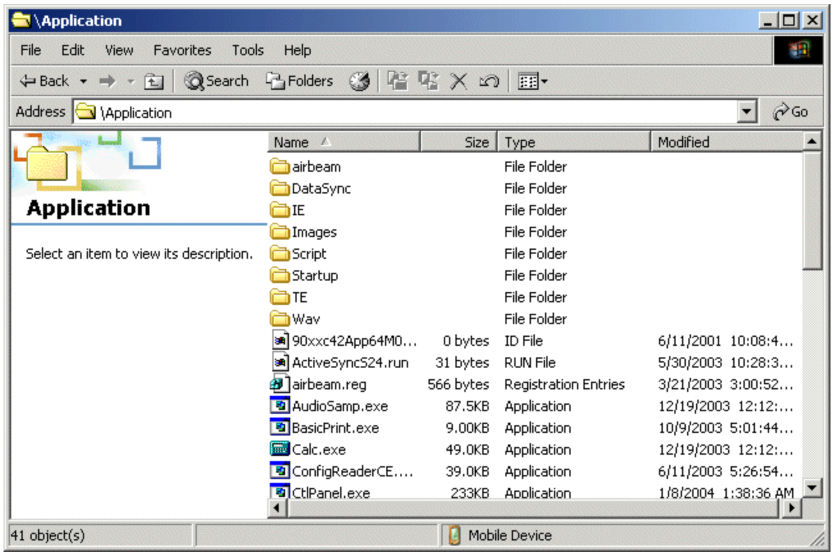

Mobile Device
File Edit View Favorites Tools Help
Back Search Folders
Address Mobile Device
Go
Mobile Device
Select an item to view its description.

Name	Size	Type	Modified
Application		File Folder	
Application Data		File Folder	
My Documents		File Folder	
Network		File Folder	
Platform		File Folder	
profiles		File Folder	
Program Files		File Folder	
Recycled		File Folder	
Temp		File Folder	
Windows		File Folder	
Control Panel	23 bytes	Shortcut	3/20/2003 8:00:03...

11 object(s) Mobile Device

Figure 4-2 *ActiveSync Explorer*

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


\Application
File Edit View Favorites Tools Help
Back Search Folders
Address \Application
Go
Application
Select an item to view its description.

Name	Size	Type	Modified
airbeam		File Folder	
DataSync		File Folder	
IE		File Folder	
Images		File Folder	
Script		File Folder	
Startup		File Folder	
TE		File Folder	
Wav		File Folder	
90xxc42App64M0...	0 bytes	ID File	6/11/2001 10:08:4...
ActiveSyncS24.run	31 bytes	RUN File	5/30/2003 10:28:3...
airbeam.reg	566 bytes	Registration Entries	3/21/2003 3:00:52...
AudioSamp.exe	87.5KB	Application	12/19/2003 12:12:...
BasicPrint.exe	9.00KB	Application	10/9/2003 5:01:44...
Calc.exe	49.0KB	Application	12/19/2003 12:12:...
ConfigReaderCE....	39.0KB	Application	6/11/2003 5:26:54...
CtlPanel.exe	233KB	Application	1/8/2004 1:38:36 AM

41 object(s) Mobile Device

Figure 4-3 *Application Folder Contents*

6. 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.
7. 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.

Adding Programs

Install the appropriate software on the host computer before installing it on the mobile computer:

1. Download the program to the host computer (or insert the CD or disk that contains the program into the host computer). The program may consist of a single *.xip file, *.exe file, a *.zip file, or a Setup.exe file.
2. Read any installation instructions, ReadMe files, or documentation that comes with the program. Many programs provide special installation instructions.
3. Connect the mobile computer to the host computer using an accessory described in *Chapter 2, Accessories*.
4. Ensure that a connection is established.
5. Double-click the executable file on the host computer.

   If the file is an installer, the installation wizard begins. Follow the directions on the window. Once the software is installed on the host computer, the installer transfers the software to the mobile computer.

   If the file is not an installer, an error message states that the program is valid but is designed for a different type of computer. Copy this file to the mobile computer. Follow the installation instructions for the program in the ReadMe file or documentation, or use ActiveSync Explore to copy the program file to the Program Files folder on the mobile computer as described in *ActiveSync on page 4-5*. For more information on copying files using ActiveSync, refer to ActiveSync Help.
6. When installation is complete, tap **Start** > **Programs** on the mobile computer, then tap the program icon.

Adding a Program from the Internet

1. Download the program to the mobile computer from the Internet using **Internet Explorer**.
2. Read any installation instructions, Read Me files, or documentation that comes with the program. Many programs provide special installation instructions.
3. Tap the file, such as a .xip or .exe file, to launch the installation wizard. Follow the directions on the window.

IPL

Use IPL to download files onto the mobile computer. See Chapter 6, Creating/Loading Hex Images to download customized flash file system partitions to the mobile computer and load hex files to the flash memory of the mobile computer.

Provisioning

Use MSP to download files onto the mobile computer and/or to transfer special software packages from a host server to the mobile computer. For more information see, *Chapter 7, Staging and Provisioning*.

SD Card (Windows CE 5.0 Only)

Use the SD card to download/upload files to and from the mobile computer. See *Secure Device Card (Windows CE 5.0 Only) on page 2-23* for more information.

Creating and Loading Hex Images

Terminal Configuration Manager (TCM) is an application used to customize flash file system partitions for the mobile computer. 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 mobile computer.

The program resident on the mobile computer 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 includes scripts used by Zebra to build the standard factory installed Platform and Application partitions provided on the mobile computer. 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 Windows CE SMDK (MC3000)\SymbolPlatforms \MC3000\TCMScripts.

✓ ***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 to the mobile computer.

✓ ***NOTE*** Screens displayed in this section are sample screens. The actual mobile computer screens may vary slightly.

Starting Terminal Configuration Manager

Click the **Start** > **Programs** > **Symbol** > **Symbol Device Configuration Packages** > **MC3000 C42V1.0** 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.

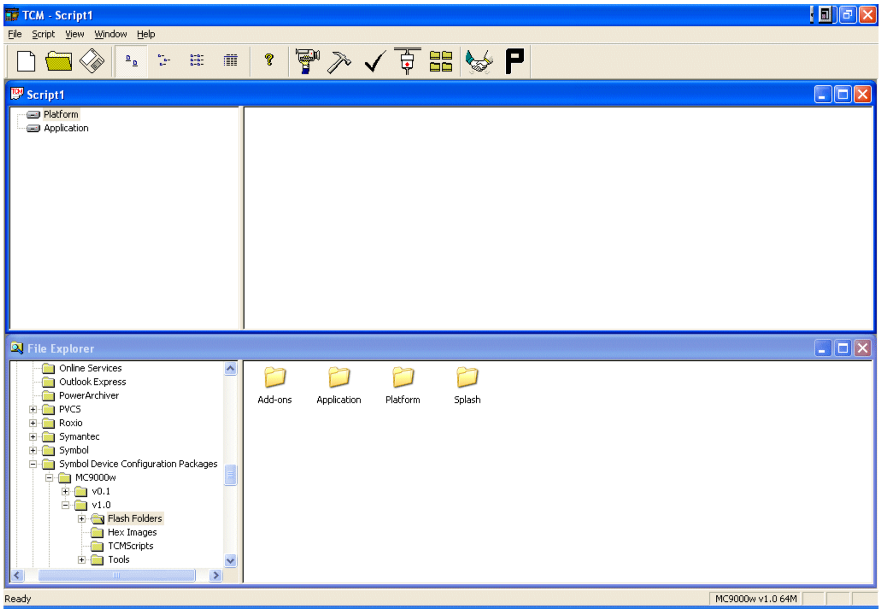


Figure 4-4 *TCM Script 1 Window*

Table 4-3 lists the TCM window components.

Table 4-3 *TCM Components*

Icon	Component	Function
Script	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.
💾	Save button	Save the current script file.
	Large icons button	View the current script items as large icons.
	Small icons button	View the current script items as small icons.

Table 4-3 *TCM Components (Continued)*

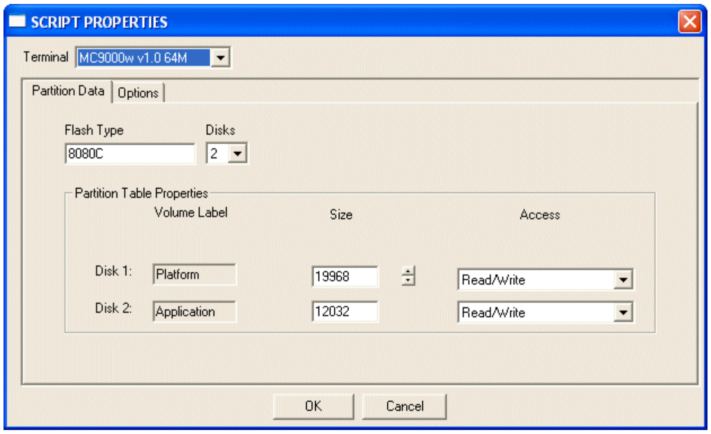
Icon	Component	Function
☰	List button	View the current script items as a list.
▤	Details button	View the current script items with more details.
?	About button	Display version information for TCM.
🎥	Properties button	View/change the current script properties.
🔨	Build button	Build the current script into a set of hex files.
✓	Check button	Check the script for errors (files not found).
🔌	Send button	Download the hex image to the mobile computer.
▦	Tile button	Arrange the sub-windows in a tiled orientation.
🤝	Build and Send button	Build the current script into a set of hex images and send the hex images to the mobile computer.
P	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 mobile computer, 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.



Terminal: MC9000w v1.0 64M

Flash Type: 8080C

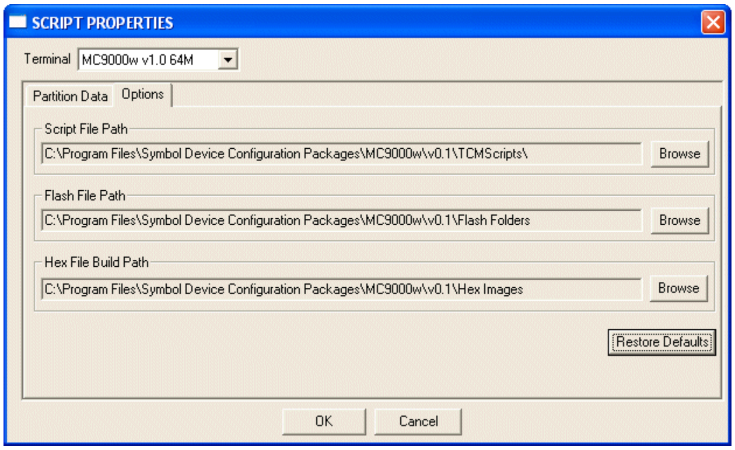
Disks: 2

Partition Table Properties

	Volume Label	Size	Access
Disk 1:	Platform	19968	Read/Write
Disk 2:	Application	12032	Read/Write

Figure 4-5 *Script Properties Window - Partition Data Tab*

3. In the **Terminal** drop-down list, the *MC3000C42a v1.0* or *MC3000C42b v1.0* entry is already selected.
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 disk partition. Note that adding space to one disk partition subtracts space 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.



Terminal: MC9000w v1.0 64M

Script File Path: C:\Program Files\Symbol Device Configuration Packages\MC9000w\v0.1\TCMScripts\

Flash File Path: C:\Program Files\Symbol Device Configuration Packages\MC9000w\v0.1\Flash Folders

Hex File Build Path: C:\Program Files\Symbol Device Configuration Packages\MC9000w\v0.1\Hex Images

Figure 4-6 *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\MC3000C42a\v0.1\TCMScripts\

\Program Files\Symbol Device Configuration Packages\MC3000C42b\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 vary. Files can be added to each of the partitions. TCM functionality includes:

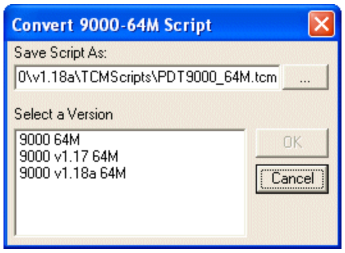
- Opening a new or existing script file
- Copying components to the script window
- Saving the script file.

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. 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, 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.



Save Script As: 0\v1.18a\TCMScripts\PDT9000_64M.tcm

Select a Version

9000 64M
9000 v1.17 64M
9000 v1.18a 64M

Figure 4-7 *Conversion Window - Upgrading to TCM 2.0*

Click on an item in the **Select a Version** list then click OK to save the script with the selected version.

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 an original or Zebra supplied standard script as a base, use the **Save As** function to save the script using a different file name.

Building the Image

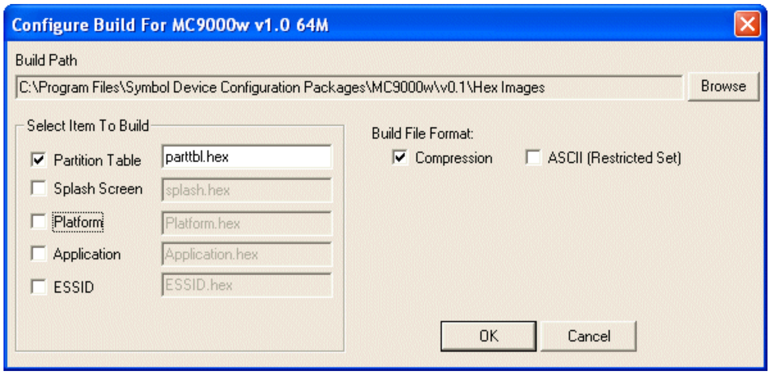
Once the script is created, the hex image defined by the script can be built.

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.

✓ ***NOTE*** The mobile computer communication must be established and external power must be provided, before resetting the mobile computer into IPL.

To build an image:

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



Configure Build For MC9000w v1.0 64M

Build Path: C:\Program Files\Symbol Device Configuration Packages\MC9000w\v0.1\Hex Images

Select Item To Build

☑ Partition Table: parttbl.hex
□ Splash Screen: splash.hex
□ Platform: Platform.hex
□ Application: Application.hex
□ ESSID: ESSID.hex

Build File Format:

☑ Compression □ ASCII (Restricted Set)

Figure 4-8 *Configure Build Window*

2. Select the items (partitions) to build using the check box(es) to the left of each named partition. The **Build Path** defines where to store all built partitions.

3. Select (hex image) Compression to reduce the size and speed up the download.

4. Click **OK** and follow the on-screen instructions.

   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.

5. 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 4-10* for more information about setting the image size appropriately.

Sending the Hex Image

Once the hex file is built, it can be downloaded to the mobile computer.

To load the hex files on to the mobile computer:

1. For downloads using either a serial or a USB connection, connect the mobile computer to the development computer using the Single Slot Serial/USB cradle or MC3000 Communication/Charge cables.

   ✓ ***NOTE*** The cradle or Communication/Charge cable must be connected with the appropriate power supplies and connected to a power source for the mobile computer to reset into IPL.

2. On the 28-key, 38-key and 48-key keypads:

   a. Press and simultaneously hold the scan button or trigger, the **1**, **9** and **Power** keys.

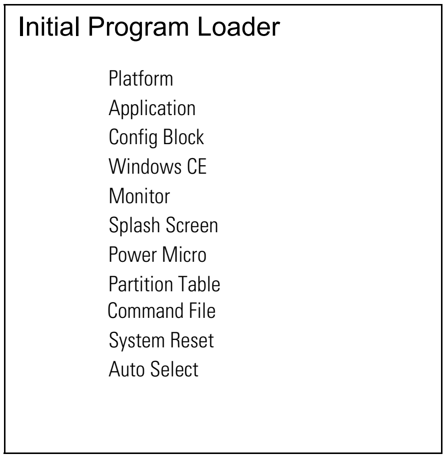
   b. Continue to hold the scan button or trigger while releasing the **1**, **9** and **Power** keys until the mobile computer resets into IPL.

3. On the 20-key keypad:

   a. Press and simultaneously hold the scan button or trigger, the **1**, **9**, **MENU** and **Fn** keys.

   b. Continue to hold the scan button or trigger while releasing the **1**, **9**, **MENU** and **Fn** keys until the mobile computer resets into IPL.

4. When the **Initial Program Loader** menu appears, release the Scan button or trigger.



Initial Program Loader

Platform
Application
Config Block
Windows CE
Monitor
Splash Screen
Power Micro
Partition Table
Command File
System Reset
Auto Select

Figure 4-9 *Initial Program Loader Menu*

⚠ ***CAUTION*** To ensure a successful download, do not remove power from the mobile computer while in IPL mode.

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

Table 4-4 *IPL Menu Partitions*

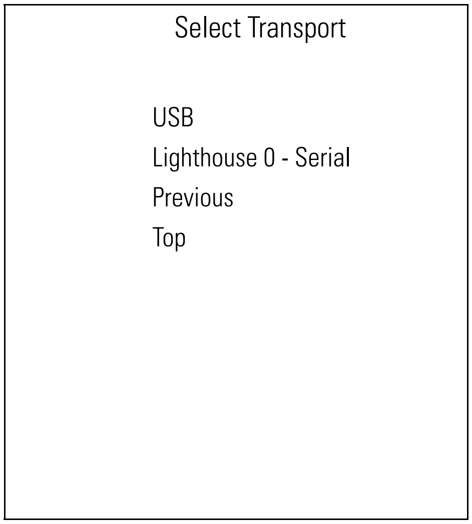
Partition Name	Description
Platform	Contains the files in the Platform folder.
Application	Contains the files in the Application folder.
Config Block	Contains information to correctly configure the operating system for the mobile computer. This information is loaded by the manufacturer. Note: Ensure that an incorrect config block is not loaded into the mobile computer. Loading an incorrect config block prevents the correct operation of the mobile computer.

Table 4-4 *IPL Menu Partitions (Continued)*

Partition Name	Description
Windows CE	Contains the operating system for the mobile computer.
Monitor	Contains the Monitor and IPL programs.
Splash Screen	Contains the splash screen that displays while booting the mobile computer. Notes: Splash screens are generated from .bmp images, (see *Splash Screen Format on page 4-22*). For mono displays, the bmp image must be 4 bits per pixel (bpp) and for color screens the color depth must be 8 bpp. 8 bpp only applies to splash screen images. Once Windows CE is running, the color density is 16 bpp.
Power Micro	The Power Micro is a small computer contained within the mobile computer 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 must be loaded first, followed by both platform and application in any order.
Command File	Displays the *Select Transport* menu, USB or Lighthouse 0 serial selection.
System Reset	Selecting this item provides a simple method to exit IPL and to cold 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 can not be used to download Monitor, Power Micro, or Partition Table. These items must be specifically selected.

✓ ***NOTE*** If the platform or application partition sizes are changed, a new partition table must be download first.

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



Select Transport

USB

Lighthouse 0 - Serial

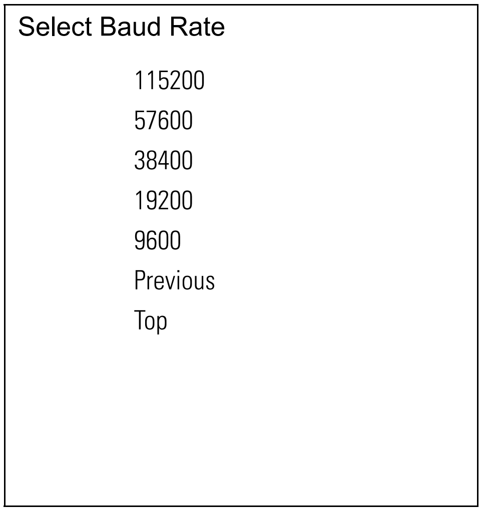
Previous

Top

Figure 4-10 *Select Transport Menu*

3. Use the up and down scroll keys to select either the **Lighthouse 0 - Serial** transport method or the **USB** transport method, then press **ENT**.

4. If the **Lighthouse 0 - Serial** transport method is selected, the **Select Baud Rate** menu appears.



Select Baud Rate

115200

57600

38400

19200

9600

Previous

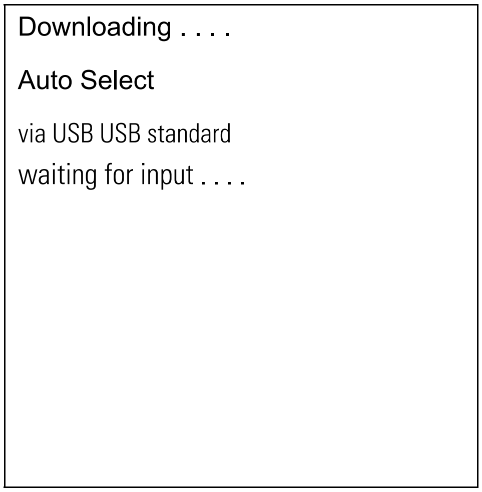
Top

Figure 4-11 *Select Baud Rate Menu*

1. Use the up and down scroll keys to select the appropriate baud rate, then press **ENT**.

2. Before the download starts, if **Serial** was selected in the **Select Transport** menu, **Waiting for Data** appears in the **Device Status** field.

3. If **USB** was selected in the **Select Transport** menu, the **Waiting for Download** message appears.



Downloading . . . .

Auto Select

via USB USB standard

waiting for input . . . .

Figure 4-12 *Waiting for Download*

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

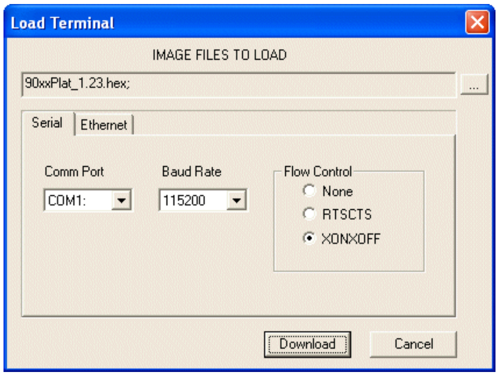


IMAGE FILES TO LOAD: 90xxPlat_1.23.hex;

Comm Port: COM1:

Baud Rate: 115200

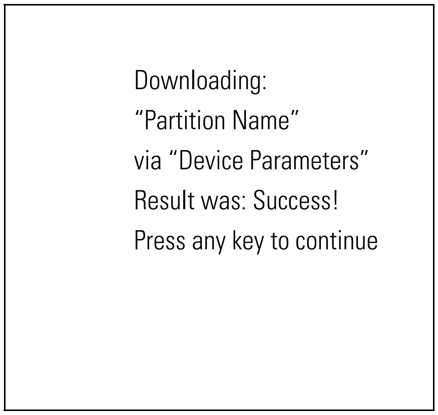
Flow Control: ○ None ○ RTSCTS ● XONXOFF

Figure 4-13 *Load Terminal Window - Serial and Ethernet Tabs*

2. For serial or USB port connections, click the **Serial** tab and select the **Image Files To Load.**

> ✓ ***NOTE*** The **USB: Zebra Device** option will not appear on the **Comm Port** drop-down list until after the **Waiting for Download** message has completed.

3. Select the **Serial** or **USB: Zebra Device** from the **Comm Port** drop-down list.
4. For serial connections, select the **Baud Rate** from the from the **Baud Rate** drop-down list.
5. Click **Download** to begin the operation.
6. During download, the **Downloading** screen on mobile computer displays the **Device Status** and a progress bar.
7. When complete, **Device Status** displays **Result was: Success!**, or in the case of an error, the cause of the error.



Downloading:
"Partition Name"
via "Device Parameters"
Result was: Success!
Press any key to continue

Figure 4-14 *Downloading Complete Screen*

1. On completion, press **ENT** to return to the **IPL** menu to select the next partition to download.
2. To exit IPL, select the **System Reset** item from the IPL menu.

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 4-5 *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.

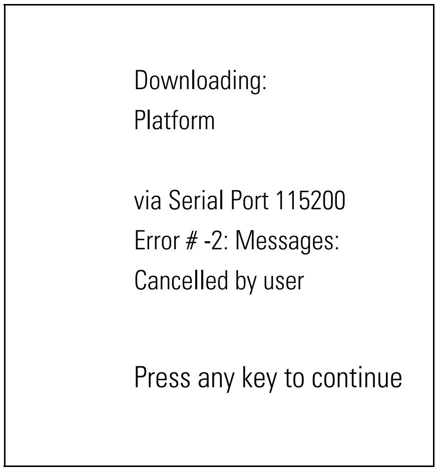
Table 4-5 *TCM Error Messages (Continued)*

Error	Description/Solution
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 mobile computer name in TCM.ini file	While loading the **Script Properties** window, TCM could not find the TCM.ini section corresponding to the mobile computer 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.
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 mobile computer, 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 mobile computer. Check if the correct flow control protocol is selected and the mobile computer 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.

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



Downloading:
Platform

via Serial Port 115200
Error # -2: Messages:
Cancelled by user

Press any key to continue

Figure 4-15 *IPL Error Screen*

This error message screen displays until a key is pressed. 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 4-6*.

Table 4-6 *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 mobile computer requires servicing.
Cancelled by user	-2	The user cancelled 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 mobile computer 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 mobile computer 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.

Table 4-6 *IPL Errors (Continued)*

Error Text	Error Number	Probable Cause
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.
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 *IPL* main menu (not Auto Select) but the file selected for download was for another partition. Ensure that the partition selected from the *IPL* 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.

Creating a Splash Screen

The source bitmap files used to create the default splash screens for the mobile computer are supplied with the DCP for MC3000 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 mobile computers with monochrome screens, open the Splashmono.bmp file supplied with the DCP for MC3000 using an image editor.
2. For mobile computers with color screens, open the Splashcolor.bmp file supplied with the DCP for MC3000 using an image editor.
3. Modify the bitmap file and save.
4. Create a splash partition using the steps in *Building the Image on page 4-13*.

Splash Screen Format

If the default files are not used to create the new splash screens, ensure to preserve the image format.

Table 4-7 *Splash Screen Format*

Screen Type	Dimensions	Bit Map File
Monochrome	320x320	4 bpp, 16 color grey scale
Color	324x324	8 bpp 256 color

See *Sending the Hex Image on page 4-13* for information about loading the splash screen using TCM and IPL.

Flash Storage

In addition to the RAM-based storage standard on Windows CE mobile computers, the mobile computer 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 mobile computer includes two FFS partitions. These partitions appear to the mobile computer 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 FFS partitions appear as two 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 mobile computer 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 mobile computer.

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” and “Platform” folders to the ActiveSync explorer. This is useful when installing applications on the mobile computer. Applications stored in the Application folder are retained even when the mobile computer is cold booted, just as the Demo 3000 program is retained in memory.

There are two device drivers included in the Windows CE image to assist developers in configuring the mobile computer 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 MC3000 contains examples of .reg files.

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

Making modifications to registry values for drivers loaded before RegMerge is not recommended. 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 mobile computer 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 MC3000. 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 mobile computer 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 mobile computer using files provided by Zebra. The current OS partition on the mobile computer is included as part of the TCM installation package. Any upgrades must be obtained from Zebra. This partition is mandatory for the mobile computer.
- Splash Screen: a bitmap smaller than 16 Kb (and limited to 8 bits per pixel) is displayed as the mobile computer cold boots. To download a customized screen to display, see *Creating a Splash Screen on page 4-21*.
- 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 mobile computer. IPL is mandatory for the mobile computer.
- Partition Table: Identifies where each partition is loaded in the mobile computer.

Downloading Partitions to the Mobile Computer

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

IPL

IPL allows the user to upgrade the mobile computer with software updates and/or feature enhancements.

Partition Update vs. File Update

There are two types of updates supported by the mobile computer: partitions and files. The file system used by the mobile computer 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 update, 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 mobile computer.

Upgrade Requirements

Upgrade requirements:

- The hex files to be downloaded (on development computer)

- A connection from the host computer and the mobile computer (either serial or wireless)
- TCM (on development computer) to download the files.

Once these requirements are satisfied, the mobile computer can be upgraded by invoking IPL and navigating the menus. See *Sending the Hex Image on page 4-13* for procedures on downloading a hex file to the mobile computer.

Chapter 5 Application Deployment for Windows Mobile 6.1

Introduction

This chapter describes new features in Windows Mobile 6.1 including new security features, how to package applications, and procedures for deploying applications onto the MC3000.

Application Design Considerations

To ensure application compatibility of a 320 x 320 display in Windows Mobile, some applications will need to be recompiled with the Microsoft WM6 SDK.

Security

The MC3000 implement a set of security policies that determine whether an application is allowed to run and, if allowed, with what level of trust. To develop an application, you must know the security configuration of the device, and how to sign an application with the appropriate certificate to allow the application to run (and to run with the needed level of trust).

Application Security

Application security controls the applications that can run on the MC3000.

- Trusted - All applications must be digitally signed by a certificate on the MC3000.
- Prompted - User is prompted to allow unsigned applications to run.
- Open - All applications run.

Developers can include their own certificates and provision the device to “trusted.”

Digital Signatures

Digital signatures provide a way to authenticate the author of EXEs, DLLs, and packages. Digitally signed applications give users confidence that an application comes from where they think it comes from. For example, if an end-user downloads an update package from the internet that is digitally signed with Zebra’s software certificate, they are assured that the package is authentic and that it was created by Zebra. By enforcing the use of digital signatures, users can also prevent malicious applications from executing on the MC3000. For example, users can provision the MC3000 to only execute “trusted” applications (digitally signed).

Zebra ships all Windows Mobile 6.1 based products in an “open” state, which means all signed and unsigned applications should work. However, customers can still reconfigure their MC3000s to operate in the “trusted” mode. This means that only applications signed with a certificate from the Privileged Execution Trust Certificate Store can run.

To support the broadest number of deployments, third-party software developers should perform the following when releasing software for a Windows Mobile 6.1 devices:

- Sign all their EXEs & DLLs with their private key
- Provide the corresponding public certificate to end-users so that it can be installed into Privileged Execution Trust Certificate Store.

If the software is installed via a .CAB file, developer should also:

- Sign the .CAB file with their private key
- Provide the corresponding public certificate to end-users so that it can be installed into SPC Certificate Store.

Locking Down a Mobile Computer

Like most configuration options in Windows Mobile 6.1, security settings are set via XML provisioning. For example, to enforce the “trusted” model and only allow applications signed with a privileged certificate to run, use the following provisioning document:

```
<wap-provisioningdoc>
<characteristic type=”SecurityPolicy”>
            <!-- Disallow unsigned apps -->
<parm name= “4102” value= “0”/>

<!-- No Prompt -->
<parm name= “4122” value= “1”/>
</characteristic>
</wap-provisioningdoc>
```

For more information on various security options, refer to the Security Policy Settings topic in the latest Windows Mobile documentation.

Installing Certificates

Use XML provisioning to query and delete certificates from certificate stores. To add a new certificate the Privileged Execution Trust Certificate Store, use the following sample provisioning document:

```
<wap-provisioningdoc>
<characteristic type= “CertificateStore”>
<characteristic type= “Privileged Execution Trust Authorities”>
<characteristic type= “657141E12FA45786F6A57CA6464032D4B3A55475”>
<parm name= “EncodedCertificate” value= “
This is sample text. This is sample text. This is sample text. This is sample text.
This is sample text. This is sample text. This is sample text. This is sample text.
This is sample text. This is sample text. This is sample text. This is sample text. = “/>
</characteristic>
</characteristic>
</characteristic>
</wap-provisioningdoc>
```

To create your own provisioning document with real certificate information:

1. Obtain a certificate from a security provider such as VeriSign.
2. Double-click on the certificate file (.CER) to open it.
3. Click on the *Details* tab and locate the *Thumbprint* field.
4. Copy the contents of the *Thumbprint* field and replace the value in the XML example above.
5. Click the **Copy to File…** button.
6. Click **Next** to start the Certificate Export Wizard.
7. Select *Base-64 encoded X.509 (.CER)* and then click **Next**.
8. Set the File Name to CertOutput.xml and click **Next**.
9. Click **Finish** to export the certificate.
10. Open the exported file, CertOutput.xml, in a text editor (i.e., NotePad).
11. Copy the contents of the file (excluding the first line, last line, and CR/LF) and replace the value of the *“EncodedCertificate”* parameter in the xml example above.

Device Management Security

You can control access to certain device settings and security levels, such as installing applications and changing security settings. Refer to the *Windows Mobile Version 6 Help* file for information on device management security.

Remote API Security

The Remote API (RAPI) enables applications that run on a desktop to perform actions on a remote device. RAPI provides the ability to manipulate the file system on the remote device, including the creation and deletion of files and directories. By default, Zebra ships with RAPI in the restricted mode. Certain tools, such as RAPIConfig, may not work properly. Refer to the *Windows Mobile Version 6 Help* file for finding information on Remote API security policies.

Packaging

✓ ***NOTE*** Applications compiled for Windows Mobile 6.1 are not backward-compatible with previous versions.

Packaging combines an application's executable files into a single file, called a package. This makes it easier to deploy and install an application to the MC3000. Package new applications and updates, such as new DLL files, as CAB files, then deploy them to Mobile 6.1 devices. Refer to the *Microsoft Windows Mobile 6 Help* file for information on CAB files.

Deployment

To install applications onto the MC3000, developers package the application and all required files into a CAB file, then load the file onto the MC3000 using one of the following options:

- Microsoft ActiveSync 4.1 or higher
- Storage Card
- MSP 3.X
- AirBEAM
- Image Update (for updating the operating system).

Refer to the *Microsoft Windows Mobile 6 Help* file for information on CAB files.

Installation Using ActiveSync

To install an application package:

- Connect the MC3000 to a host computer using ActiveSync. See *Chapter 3, ActiveSync* for more information.
- Locate the package file on the host computer.
- In ActiveSync on the host computer, open *Explorer* for the MC3000.
- Copy the CAB file from the host computer to the \temp directory on the MC3000.
- On the MC3000, navigate to the \temp directory.
- Tap on the application CAB file. The application installs on the MC3000.

Installation Using AirBEAM

See *Chapter 7, Staging and Provisioning* for information on AirBEAM.

MSP 3.X

See *Chapter 7, Staging and Provisioning* for information on MSP3.X.

Image Update

Windows Mobile 6.1 contains an Image Update feature that updates all operating system components. All updates are distributed as update packages. 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.

To update an operating system component, copy the update package to the MC3000 using one of a variety of transports, including ActiveSync and MSP. Then, initiate the update using one of the following methods:

- Double-tap the package file in **File Explorer** (similar to extracting a CAB file)
- Perform a special boot sequence that initiates the update.

✓ ***NOTE*** The MC3000 must have at least 5 MB of free space to perform an OS update.

To initiate an update:

1. Go to the Support Central web site, http://www.zebra.com/support.
2. Download the appropriate update package.
3. Copy the update package to the \temp directory on the MC3000.
4. Connect the MC3000 to AC power. See *Chapter 2, Accessories*.
5. Simultaneously press the **Power** button and the **1** and **9** keys.
6. Immediately, as soon as the device starts to boot and before the splash screen is visible, press and hold the left scan button.
7. The Update Loader application first looks for a file in the \temp directory.

   When it finds the appropriate file, it loads the package onto the MC3000. A progress bar displays until the update completes.
8. The MC3000 re-boots.
9. The calibration screen appears.

✓ ***NOTE*** When initiating an update via a boot sequence, the update loader looks for updates in the root of the \temp folder on the MC3000's persistent storage volume. A response file, pkgs.lst, indicates which files to update. In most cases, Zebra provides this pkgs.lst file with the update and you should only modify it when updating a splash screen partition. See *Creating a Splash Screen* for more information.

Creating a Splash Screen

Use a bitmap file to create a customized splash screens for the MC3000. Use Image Update with a bitmap file, rather than a package file, to update the splash screen.

To create a custom splash screen:

1. Create a .bmp file using a graphic program with the following specifications:
   - Size: 320 (W) x 240 (H).
   - Colors: 16 bits per pixel (65536 colors) for color displays.
2. Modify the bitmap file and save.

To load the splash screen on the MC3000:

1. Create a text file named pkgs.lst which contains the name of the bmp file. For example, *mysplash.bmp*.
2. Copy the bmp file and the pkgs.lst file to one of the following:
   - MC3000’s \temp directory
   - MC3000’s \Windows directory.
3. Perform a cold boot.
4. Press the trigger or side scan button for 5 seconds while booting to invoke the Update Loader and install the splash screen.

XML Provisioning

To configure the settings on an MC3000, use XML provisioning. To install an XML provisioning file on the MC3000, create a Cabinet Provisioning File (CPF). A CPF file is similar to a CAB file and contains just one file: _setup.xml. Like a CAB file, the CPF extension is associated with WCELoad.EXE. Opening a CPF extracts the XML code and uses it to provision and configure the MC3000. The user receives an e-mail notification indicating success or failure.

XML provisioning provides the ability to configure various features of the MC3000 (i.e., registry and file system). However, some settings require security privileges. To change registry settings via a CPF file, you must have certain privileges (roles). Some registry keys require you to simply be an *Authenticated User*, while other registry keys require you to be a *Manager*. Refer to the *Microsoft Windows Mobile 6 Help* file, *Metabase Settings for Registry Configuration Service Provider* section, for the default role settings in Windows Mobile 6.1.

For those registry settings that require the *Manager* role, the CPF file must be signed with a privileged certificate installed on the device. Refer to the *Microsoft Windows Mobile 6 Help* file and the *Windows Mobile 6 SDK* for instructions and sample test certificates.

Creating an XML Provisioning File

To create a .cpf file:

1. Create a valid provisioning XML file named _setup.xml using an XML editor or the tools supplied with Visual Studio 2005. (For example, use the SampleReg.xml sample created in the *RegMerge* section and rename it _setup.xml.) Ensure the file contains the required parameters for the operation. Refer to the *Microsoft Windows Mobile 6 Help* file for information.
2. In the Windows Mobile 6.1 tools directory on the desktop computer (typically \Program Files\Windows CE Tools\wce500\Windows Mobile 6 Pocket PC SDK\Tools), run the Makecab.exe utility, using the following syntax to create a .cpf file from the _setup.xml file:

   ```
   MakeCab.exe /D COMPRESS=OFF _setup.xml myOutCpf
   ```

✓ ***NOTE*** COMPRESS=OFF is required for backward compatibility with Pocket PC.

3. Optionally, use the Authenticode tools to sign the .cpf file.
4. Tap the filename to install.
5. Certain applications and settings require a cold boot to take affect. In these cases, cold boot the MC3000. Refer to the *Windows Mobile Version 6 Help* file for more information.

XML Provisioning vs. RegMerge and Copy File

Prior to Windows Mobile 6.1, Zebra used two drivers (RegMerge and CopyFiles) to update the registry and to copy files during a cold boot. With Mobile 6.1, Zebra recommends using XML provisioning instead. RegMerge and CopyFiles are supported for backward compatibility but Zebra may eliminate support in the future. The following sections provide examples of how RegMerge and CopyFiles were used, and how to perform the same function using XML provisioning.

RegMerge

RegMerge.dll is a built-in driver that allows updating the registry during a clean boot. RegMerge runs very early in the boot process and looks for registry files (.reg files) in certain Flash File System folders (i.e., \Application) during a clean boot. It then merges the registry changes into the system registry located in RAM.

The following example uses RegMerge to set a registry key:

SampleReg.reg

```
[HKEY_LOCAL_MACHINE\Hardware\DeviceMap\Backlight]
“BacklightIntensity”=dword:00000036
```

The following example uses XML provisioning to perform the same task:

SampleReg.xml

```
<wap-provisioningdoc>
    <characteristic type= “Registry”>
        <characteristic type= “HKLM\Hardware\DeviceMap\Backlight”>
            <parm name= “BacklightIntensity” value= “54” datatype= “integer” />
        </characteristic>
    </characteristic>
</wap-provisioningdoc>
```

CopyFiles

CopyFiles copies files from one folder to another on a clean boot. During a clean boot CopyFiles looks for files with a .CPY extension in the root of the Application FFS partition. These files are text files containing the source and destination for the desired files to copy, separated by “>”.

The following example uses CopyFiles to copy a file from the \Application folder to the \Windows folder:

SampleCpy.cpy

```
\Application\example.txt > \Windows\example.txt
```

The following example uses XML provisioning to perform the same task:

SampleCpy.xml

```
<wap-provisioningdoc>
    <characteristic type= “FileOperation”>
        <characteristic type= “\Windows” translation= “filesystem”>
            <characteristic type= “MakeDir”/>
            <characteristic type= “example.txt” translation= “fileystem”>
                <characteristic type= “Copy”>
                    <parm name= “Source” value= “\Application\example.txt” translation= “filesystem”/>
                </characteristic>
            </characteristic>
        </characteristic>
    </characteristic>
</wap-provisioningdoc>
```

Storage

Mobile 6.1 contains three types of file storage:

- Random Access Memory (RAM)
- Persistent Storage
- Application folder.

Random Access Memory

Executing programs use RAM to store data. Data stored in RAM is lost upon a warm boot. RAM also included a volatile file storage area called *Cache Disk*.

Volatile File Storage (Cache Disk)

Windows Mobile 6.1 memory architecture uses persistent storage for all files, registry settings, and database objects to ensure data is retained even after a power failure. Persistent storage is implemented using Flash memory technology which is generally slower than volatile RAM memory. In certain situations the speed of the operation is more important than the integrity of the data. For these situations, Zebra has provided a small volatile File Storage volume, accessed as the *Cache Disk* folder. Disk operations to the *Cache Disk* folder are much faster than to any of the persistent storage volumes, but data is lost across warm boots and power interruptions. Note that a backup battery powers RAM memory, including the *Cache Disk*, when you remove the main battery for a short period of time.

The MC3000 uses the *Cache Disk* for temporary data that can be restored from other sources, for example, for temporarily “caching” HTML web pages by a browser or generating formatted files to send to a printer. Both situations benefit from the increased speed of the cache disk, but you can restore the data if needed.

DO NOT use the *Cache Disk* as a method to improve application performance. Analyze applications that perform slower in persistent storage to optimize disk access. Common areas for optimization include minimizing the number of reads and writes to a file, removing unneeded debug logging, and minimizing file flushing or closing files.

Persistent Storage

Windows Mobile 6.1 protects all data and applications from power-related loss. Because Windows Mobile 6.1 mounts the entire file system and registry in persistent storage (rather than using RAM), MC3000 devices provide a reliable storage platform even in the absence of battery power.

Persistent storage provides application developers with a reliable storage system available through the standard file system and registry APIs. Persistent storage is optimized for large reads and writes; therefore, applications reading and writing data in large chunks tend to outperform those applications reading and writing small blocks of data. Data in persistent storage is lost upon a clean boot.

Persistent storage contains all the directories under the root directory except for Application, Cache Disk, and Storage Card (if a storage card is installed). Persistent storage is approximately 60 MB (formatted).

Application Folder

The Application folder is a super-persistent storage that is persistent even after a clean boot. Accessing data in the Application folder is slower than accessing persistent storage. The Application folder is used for deployment and device-unique data. For example, network profiles can be stored in the Application folder so that connection to the network is available after a cold boot. The Application folder is approximately 20 MB (formatted).

Device Configuration Manager

Device Configuration Manager (DCM) is a utility that runs on the development computer and is used to create configuration files. These files, when deployed to an MC3000, set configuration parameters for that device. The configurable options for a MC3000 are defined in an XML file that is available on the Support Central (http://www.zebra.com/support) for that MC3000. SCM is also available on Support Central.

SCM eliminates the potential user errors that occur when manually editing registry settings.

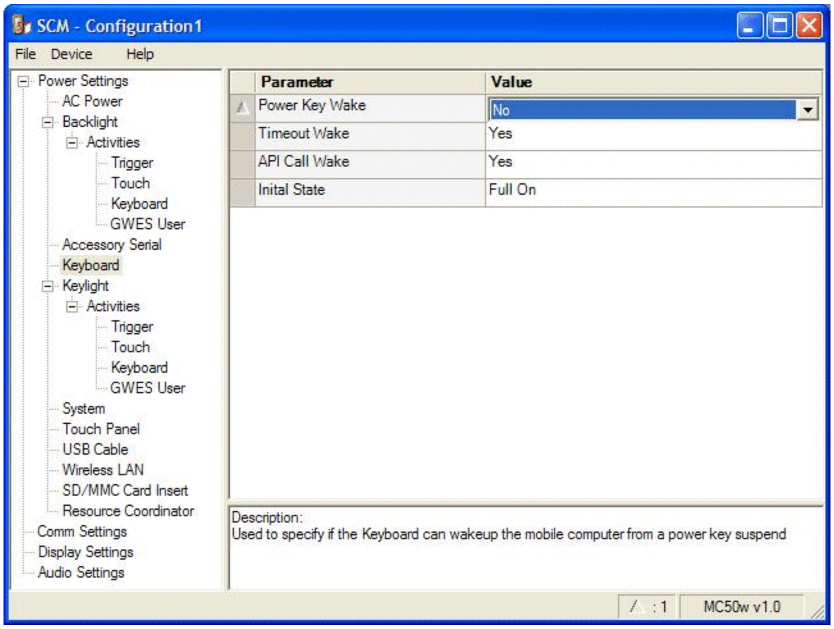
File Types

SCM uses three types of files:

- Device Configuration Template (.DCT) files are XML files that define the configurable parameters for a device.
- Registry Configuration Service Provider XML files for device provisioning.
- CAB Provisioning Format (.CPF) file which is a .CAB archive that contains the provisioning XML. This file is downloaded to the MC3000 and merged upon a cold boot.

User Interface

SCM's user interface consists of a tree control on the left side of the window which displays all the configuration categories, and a data grid table on the right which displays all the configurable controls for the selected category. *Figure 5-1* shows the main window for a device’s .sct file.



Parameter	Value
Power Key Wake	No
Timeout Wake	Yes
API Call Wake	Yes
Inital State	Full On

Description:
Used to specify if the Keyboard can wakeup the mobile computer from a power key suspend

Figure 5-1 *Main SCM Window*

Menu Functions

Use the main menu to access the program functionality described in *Table 5-1*.

Table 5-1 *SCM Menu Functions*

Menu Item	Description
File Menu	
Open Config File	Open a saved configuration file (.SCD).
Save Config Changes	Save changes to the currently loaded configuration file.
Restore All Defaults	Restore all parameter values to the default state. The default values are stored in a Device Configuration template file (i.e., MC3000w.sct).
Export Changes to .xml	Export the changed parameter values to an XML file.
Export Changes to .cpf	Export the changed parameter values to an CPF file.
Export all to .xml	Export all the parameter values to an XML file.
Export all to .cpf	Export all the parameter values to an CPF file.
Exit	Exit Device Configuration Manager.
Device Menu	
Device type	Change the current device type template. Each template (available from the Support Central) must reside in the SCM directory.
Help Menu	
About	Display the *About* dialog which shows the application version.

Parameter State Indicators

The first column of the data table displays parameter state indicators. The state indicators display one of the states in *Table 5-2* for a particular parameter:

Table 5-2 *Parameter Status Indicators*

Icon	Indicator	Description
△	Modified	This parameter was changed from its initial factory setting.
🚫	Invalid	This parameter is not valid for the selected device type. This can occur when a configuration file for one type of device is loaded and the device type is changed using the *Device* menu. Values marked “invalid” are not included in an exported.

Window Status Bar

The SCM status bar found on the bottom right corner of the window contains the items in *Table 5-3* from left to right:

Table 5-3 *Window Status Bar Items*

Status Bar Item	Description
Invalid Count	Number of parameters not valid for the selected device.
Modified Count	Number of parameters modified from the factory defaults.
Device Type	Device type - version.

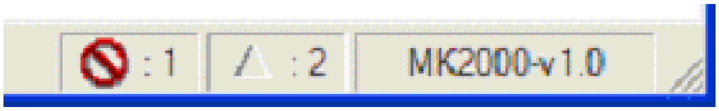


Figure 5-2 *Sample Status Bar*

The sample status bar in *Figure 5-2* shows that the current configuration file contains 1 Invalid Parameter and 2 Modified Parameters.

File Deployment

The CPF file created by the SCM export function must be deployed to the MC3000.

1. Optionally, use the Authenticode tools to sign the .cpf file.
2. Make the .cpf file read-only, then copy it to the MC3000.
3. Tap the filename to install.
4. Certain applications and settings require a cold boot to take affect. In these cases, cold boot the MC3000. Refer to the *Windows Mobile Version 6 Help* file for more information.

Enterprise Mobility Developer Kits

The Enterprise Mobility Developer Kit (EMDK) family of products allows you to write applications that take advantage of the capture, move and manage capabilities of the MC3000. Go to the Support Central (http://www.zebra.com/support) to download the appropriate developer kit.

Chapter 6 Wireless Applications

Introduction

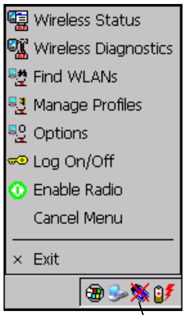
✓ *NOTE* This chapter provides information for Wireless Applications up to version 2.5. For later versions, refer to the Wireless Fusion Enterprise Mobility Suite User Guide for Version X.XX, where X.XX is the version number. Go to http://www.zebra.com/support for the latest user guide.

Wireless LANs allow mobile computers to communicate wirelessly and to send captured data to a host device in real time. Before a mobile computer can be used on a Spectrum24 WLAN, the facility must be set up with the required hardware to run the wireless LAN and the mobile computer must be properly configured. Refer to the documentation that came with the Access Points (APs) for instructions on setting up the hardware.

To configure the mobile computer, a set of wireless applications provide the user with the tools to configure and test the wireless radio embedded the mobile computer. The following wireless applications are available on the task tray from the **Wireless Application** menu:

- Wireless Status
- Wireless Diagnostics
- Find WLANs
- Manage Profiles
- Options
- Log On/Off
- Enable/Disable Radio (Fusion 2.5 only).

Tap the **Signal Strength** icon to display the **Wireless Application** menu.



Signal Strength Icon

Figure 6-1 *Wireless Applications Menu*

Signal Strength Icon

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

Table 6-1 *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. Notify the network administrator.

Turning Off the Radio

On Device with Windows CE 5.0 (OEM Version 01.15 or lower)

NOTE To determine the operating system OEM version, see *Configurations on page xii*.

To turn off the WLAN radio:

1. Tap **Start** > **Settings** > **Control Panel** > **Power** icon > **PwrDevices** tab.
2. In the text box, scroll down until **WLP1**: displays.
3. Select **WLP1**:. **WLP1:** displays in the text box at the top of the window.
4. In the drop-down list box, select **D4**.
5. Tap **Set**.

To turn on the radio:

1. Tap **Start** > **Settings** > **Control Panel** > **Power** icon > **PwrDevices** tab.
2. In the text box, scroll down until **WLP1**: displays.
3. Select **WLP1**:. **WLP1:** displays in the text box at the top of the window.
4. In the drop-down list box, select **D0**.
5. Tap **Set**.

On Device with Windows CE 5.0 (OEM Version 01.16 or higher)

NOTE To determine the operating system OEM version, see *Configurations on page xii*.

To turn off the WLAN radio tap the **Wireless Connection Status** icon on the task tray and select **Disable Radio**. A red X appears across the icon indicating that the radio is disabled (off).

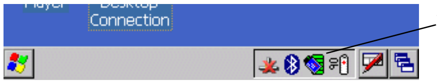


Figure 6-2 *Wireless Connection Status Icon*

To turn the radio back on, tap the **Wireless Connection Status** icon on the task tray and select **Enable Radio**. The red X disappears from the icon indicating that the radio is enabled (on).

Bluetooth Radio

To turn off the Bluetooth radio, tap **Bluetooth** icon in the task tray and select **Disable Bluetooth**.

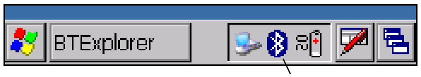


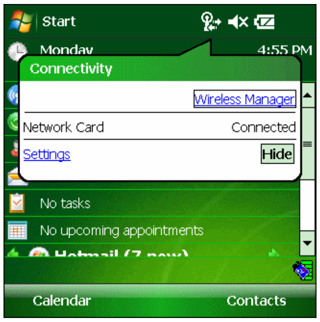
Figure 6-3 *Bluetooth Icon*

To turn on the Bluetooth radio, tap **Bluetooth** icon in the task tray and select **Enable Bluetooth**.

On Device with Windows Mobile 6.1

Windows Mobile 6.1 devices include **Wireless Manager**, which provides a simple method of enabling, disabling the WLAN radio.

To open **Wireless Manager**, tap the **Connectivity** icon.



Network Card Connected

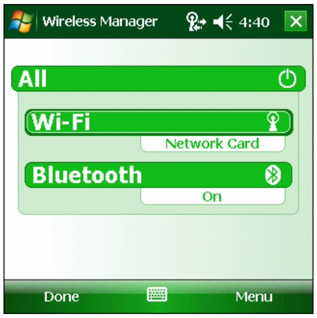
No tasks

No upcoming appointments

Hotmail (7 new)

Figure 6-4 *Opening Wireless Manager*

Select **Wireless Manager**.



Wi-Fi: Network Card

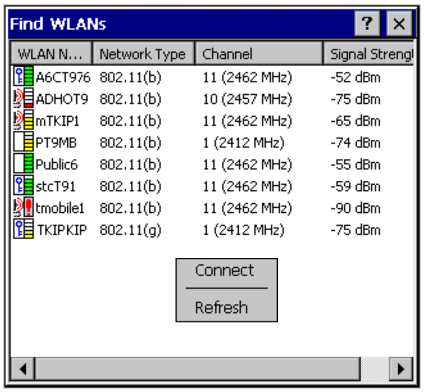
Bluetooth: On

Figure 6-5 *Wireless Manager Window*

To enable or disable the WLAN radio, tap the Wi-Fi bar.

Find WLANs Application

Use the **Find WLANs** application to discover available networks in the vicinity of the user and mobile computer. To open the **Find WLANs** application, tap the **Signal Strength** icon > **Find WLANs**. The **Find WLANs** window displays.



Find WLANs

WLAN N...	Network Type	Channel	Signal Strengt
A6CT976	802.11(b)	11 (2462 MHz)	-52 dBm
ADHOT9	802.11(b)	10 (2457 MHz)	-75 dBm
mTKIP1	802.11(b)	11 (2462 MHz)	-65 dBm
PT9MB	802.11(b)	1 (2412 MHz)	-74 dBm
Public6	802.11(b)	11 (2462 MHz)	-55 dBm
stcT91	802.11(b)	11 (2462 MHz)	-59 dBm
tmobile1	802.11(b)	11 (2462 MHz)	-90 dBm
TKIPKIP	802.11(g)	1 (2412 MHz)	-75 dBm

Figure 6-6 *Find WLAN Window*

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

Valid ESSIDs that were not displayed in the Find WLAN Window may be entered manually. See *Figure 6-7 on page 6-6*.

The **Find WLANs** list displays:

- WLAN Networks - Available wireless networks with an icon that indicates signal strength and encryption type. The signal strength and encryption icon is described in tables *Table 6-2* and *Table 6-3*.
- Network Type - Type of network.
- Channel - Channel that the AP is transmitting on.
- Signal Strength - Displays the signal strength of the signal from the AP.

Table 6-2 *Signal Strength Icon*

Icon	Description
🟩	Excellent signal
🟩	Very good signal
🟨	Good signal
🟨	Fair signal
🟥	Poor signal
❗	Out of range or no signal

Table 6-3 *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.

Tap-and-hold on a WLAN network to launch a context sensitive menu. The menu provides two options: **Connect** and **Refresh**. Select **Refresh** to refresh the WLAN list. Wireless profiles may also be created from one of the listed networks by selecting a network from the list and then selecting **Connect**. Selecting **Connect** displays the **Profile Editor Wizard**. The wizard is initialized to set the values for the selected network. After the profile editing is completed, it automatically connects to the newly edited profile.

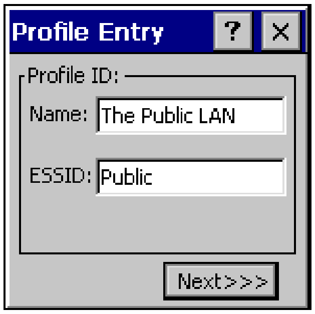
Profile Editor Wizard

The **Profile Editor Wizard** displays when creating a new profile, or editing an existing profile. If editing a profile, the fields are populated with the current settings for that profile. If creating a new profile, the known information for that WLAN network are populated into the fields.

Navigate through the wizard using the **Next** and **Back** buttons. Tap **X** to quit, a notification box appears asking the user to confirm the quit. Tap **No** to return to the wizard or tap **Yes** to quit and return to the **Manage Profiles** window.

Profile ID

The **Profile ID** dialog box is the first dialog box in the **Profile Editor Wizard**. Use the **Profile ID** dialog box to input the fields for the profile name and the ESSID.



Profile ID:

Name: The Public LAN

ESSID: Public

Figure 6-7 *Profile ID Dialog Box*

Table 6-4 *Profile ID Fields*

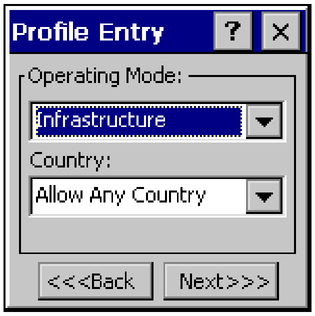
Field	Description
Name	Populated with the name and (WLAN) identifier of the network connection. Use the *Name:* field to enter a user friendly name of the mobile computer profile used to connect to either an AP or another networked computer. Example: The Public LAN.
ESSID	The ESSID is the 802.11 extended service set identifier. The ESSID is 32-character (maximum) string identifying the WLAN. The ESSID assigned to the mobile computer is required to match the AP ESSID for the mobile computer to communicate with the AP.

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

Tap **Next**. 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.


Profile Entry

Operating Mode: Infrastructure

Country: Allow Any Country

Figure 6-8 *Operating Mode Dialog Box*

Table 6-5 *Operating Mode Fields*

Field	Description
Operating Mode	Infrastructure: Select **Infrastructure** to enable the mobile computer to transmit and receive data with an AP. Infrastructure is the mobile computer default mode. Ad Hoc: Select **Ad Hoc** to enable the mobile computer to form its own local network where mobile computers communicate peer-to-peer without APs using a shared ESSID.
Country	Country: is used to determine 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. Single Country Use: When the device is only to be used in a single country, set every profile country to **Allow Any Country**. In the **Options** > **Regulatory** dialog box (see *Figure 6-46 on page 6-38)*, set the country to the specific country the device is to be used in, and deselect (uncheck) the Enable 802.11d option. This is the most common and the efficient configuration. It eliminates the initialization overhead associated with acquiring a country via 802.11d. Multiple Country Use: When the device may be used in more than one country, select (check) the *Enable 802.11d* option in the **Regulatory Options** dialog box (see *Figure 6-46 on page 6-38)*. This eliminates the need for reprograming the country (in **Options** > **Regulatory**) each time a new country is entered. However, this only works if the infrastructure (i.e. APs) support 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. 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. 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.

Tap **Next**. 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 6-9* for instruction on setting up authentication.

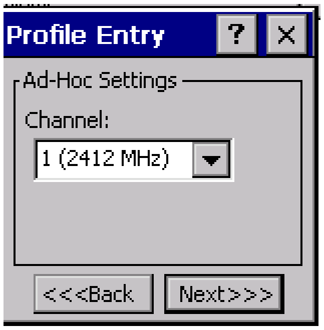
Ad-Hoc

Use the **Ad-Hoc** dialog box to select the necessary information to control **Ad-Hoc** mode. This dialog box does not display if **Infrastructure** mode is selected. To select Ad-Hoc mode:

1. Select a channel number from the **Channel** drop-down list.

Table 6-6 *Ad-Hoc Channels*

Band	Channel	Frequency
2.4 GHz	1	2412 MHz
	2	2417 MHz
	3	2422 MHz
	4	2427 MHz
	5	2432 MHz
	6	2437 MHz
	7	2442 MHz
	8	2447 MHz
	9	2452 MHz
	10	2457 MHz
	11	2462 MHz
5 GHz	36	5180 MHz
	40	5200 MHz
	44	5220 MHz
	48	5240 MHz



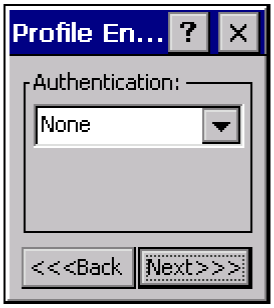
Channel: 1 (2412 MHz)

Figure 6-9 *Ad-Hoc Settings Dialog Box*

2. Tap **Next**. The **Authentication** dialog box displays.

Authentication

Use the **Authentication** dialog box to configure authentication. If **Ad-Hoc** mode is selected, this dialog box is not available and authentication is set to None by default. *Table 6-7* lists the available authentication options.



Authentication:

None

Figure 6-10 *Authentication Dialog Box*

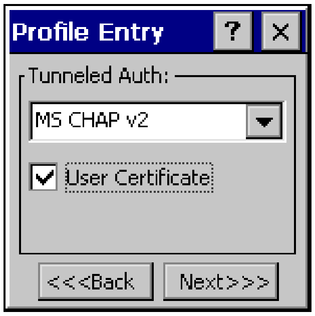
Table 6-7 *Authentication Options*

Authentication	Description
None	Default setting when authentication is not required on the network.
EAP-TLS	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. EAP TLS achieves this through 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. LEAP is founded on mutual authentication. The AP and the mobile computer attempting to connect to it require authentication before access to the network is permitted.
TTLS	Select this option to enable TTLS authentication.

Select an authentication type from the drop-down list and tap **Next**. If **PEAP** or **TTLS** is selected, the **Tunneled** dialog box displays. If **None**, **EAP TLS** or **LEAP** is selected the **Encryption** dialog box displays. See *Encryption on page 6-18* for encryption options.

Tunneled Authentication

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



Tunneled Auth:

MS CHAP v2

☑ User Certificate

Figure 6-11 *Tunneled Auth Dialog Box*

1. Tap a tunneled authentication type from the drop-down list.

2. Select the **User Certificate** check box if a certificate is required. The TLS tunnel type requires a user certificate, so the check box is automatically selected.
3. Tap **Next**. The **Installed User Certs** dialog box appears.

Table 6-8 lists the PEAP tunneled authentication options.

Table 6-8 *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 the phase 2 of the authentication process. This method uses a user certificate to authenticate.

Table 6-9 lists the TTLS tunneled authentication options.

Table 6-9 *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 has been 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. In most respects, MS CHAP is identical to CHAP, but there are a few differences. 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 6-9 *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 the **User Certificate** check box on the **Tunneled Authentication** dialog box is checked or if **TLS** is the selected authentication type, then the **Installed User Certificates** dialog box displays. The user is required to select a certificate before proceeding. Select a certificate from the drop-down list of currently installed certificates. When a certificate is selected its name appears in the drop-down list. If the required certificate is not in the list, it must be installed.

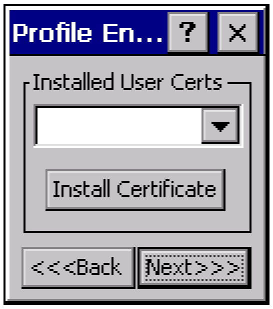
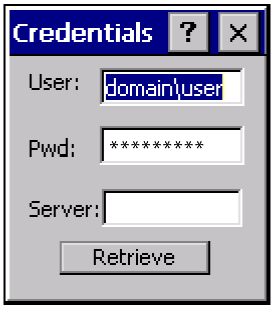


Figure 6-12 *Installed User Certs Dialog Box*

User Certificate Installation

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

1. Tap **Install Certificate**. The **Credentials** dialog box appears.



User: domain\user

Pwd: *********

Figure 6-13 *Credentials Dialog Box*

2. Enter the **User:**, **Pwd:** (password), and **Server:** information in their respective text boxes.

3. Tap **Retrieve**. A **Progress** dialog appears to indicate the status of the certificate retrieval.

4. Tap **ok** to exit.

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

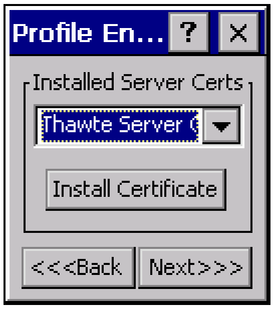
✓ ***NOTE*** In order to successfully install a user certificate, the mobile computer must already be connected to a network from which the server is accessible.

Server Certificate Selection

If the **Validate Server Cert** check box is checked, a server certificate is required. The wizard displays the **Installed Server Certs** dialog box and a certificate must be selected before proceeding. An hour glass may be displayed as the wizard populates the existing certificate list. If the required certificate is not listed, then it must be installed.

To select a certificate:

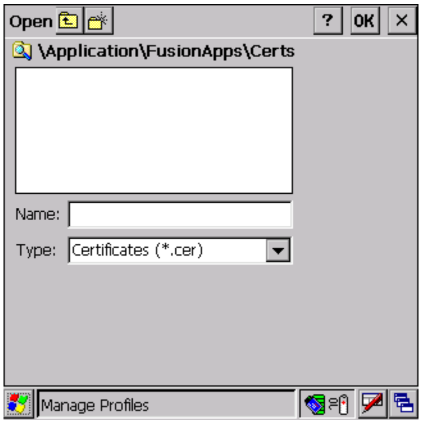
1. Tap the **Install Certificate** button to install a certificate.



Installed Server Certs: Thawte Server C

Figure 6-14 *Installed Server Certs Dialog Box*

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



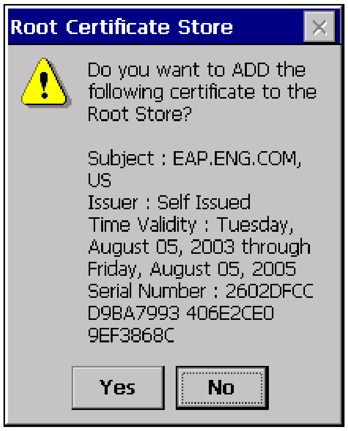
\Application\FusionApps\Certs

Name:

Type: Certificates (*.cer)

Figure 6-15 *Browse Server Certificates*

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



Root Certificate Store

Do you want to ADD the following certificate to the Root Store?

Subject : EAP.ENG.COM, US
Issuer : Self Issued
Time Validity : Tuesday, August 05, 2003 through Friday, August 05, 2005
Serial Number : 2602DFCC D9BA7993 406E2CE0 9EF3868C

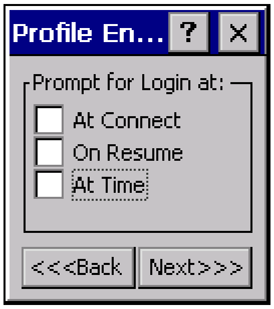
Figure 6-16 *Confirmation Dialog Box*

Credential Cache Options

If any of the password based authentication types are chosen, then different credential caching options may be specified. These options allow an administrator to specify when the network credentials prompts appear. The network credentials prompts can be set to appear; at connection, on each resume, or at a specified time.

An administrator can enter the credentials directly into the profile which permanently caches the credentials. In this case, user login to the mobile computer is not required. If a profile does not contain credentials entered through the configuration editor, then the user must login to the mobile computer before connecting.

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



Prompt for Login at:

□ At Connect
□ On Resume
□ At Time

Figure 6-17 *Prompt for Login at Dialog Box*

If mobile computer does not have the credentials, the user is prompted to enter a username and password. If the mobile computer has the credentials (previous entered via a login dialog box), it uses these credentials unless the caching options require the mobile computer to prompt for new credentials. If the credentials were entered via the profile, the mobile computer does not prompt for new credentials. *Table 6-10* lists the caching options.

Table 6-10 *Cache Options*

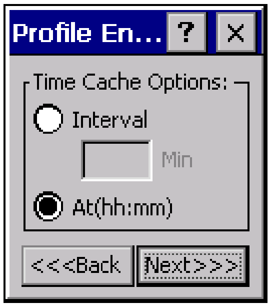
	Description
At Connect	If this option is selected, then a user is prompted for credentials whenever the WCS tries to connect to a new profile. If this option is not set, then the cached credentials are used to authenticate. If the credentials are not cached, then the user is prompted to enter credentials. This option only applies if a user is logged in.
On Resume	If the **On Resume** option is selected, an authenticated user is reauthenticated when a suspend/resume occurs. Once the user is reauthenticated, the user is prompted for credentials. If the user does not enter the same credentials that were entered prior to the suspend/resume, the user is disconnected from the network. The user may try up to three times to enter the correct credentials. If the correct credentials are entered, then the network connection remains intact. This option only applies if a user is logged in.
At Time	Use 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, the times should be at least 5 minutes intervals. Once the time has passed, the user is prompted for credentials. If the user enters the correct credentials, the network connection remains intact. If the user enters the wrong credentials, the user is disconnected from the network. The user may try up to three times to enter the correct credentials. If the correct credentials are entered, then the network connection remains intact. This option only applies if a user is logged in.

When a user enters the credentials, the credentials are applied to a particular profile. If a user logs out, all of the cached credentials are cleared. If a profile is edited, then all cached credentials for that profile are cleared.

The following authentication types have credential caching:

- EAP TLS
- PEAP
- LEAP
- TTLS.

If the **At Time** check box is selected the **TIme Cache Options** dialog box displays.



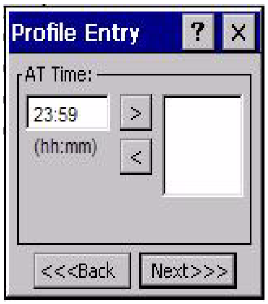
Time Cache Options:

○ Interval

● At(hh:mm)

Figure 6-18 *Time Cache Options Dialog Box*

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



AT Time:

23:59

(hh:mm)

Figure 6-19 *At Time Dialog Box*

6. Enter the time using the 24 hour clock format in the **(hh:mm)** box.
7. Tap **>** to move the time to the right. Repeat for additional time periods.
8. Tap **Next**. 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.

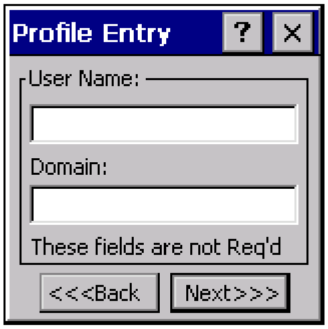


Figure 6-20 *Username Dialog Box*

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.

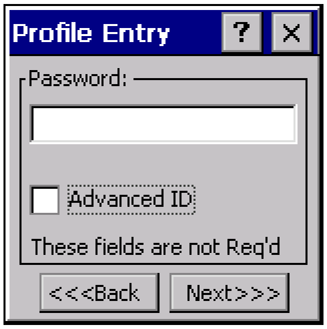


Figure 6-21 *Password Dialog Box*

1. Enter a password in the **Password** field.

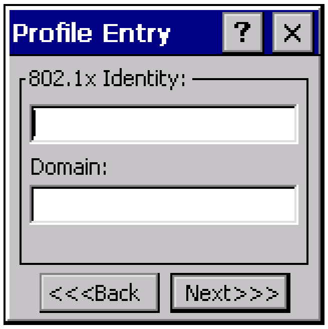
2. Select the **Advanced ID** check box, if advanced identification is required.

3. Tap **Next**, the **Encryption** dialog box displays. See *Encryption on page 6-18* for setting the encryption information.

Advanced Identity

Use the **Advanced ID** dialog box to enter the 802.1X identity. The 802.1X identity value can be 63 characters long and is a case sensitive identity supplied to the authenticator. In TTLS and PEAP, it is recommended that this field not contain a true identity, but instead the identity **anonymous**, 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.



Profile Entry

802.1x Identity:

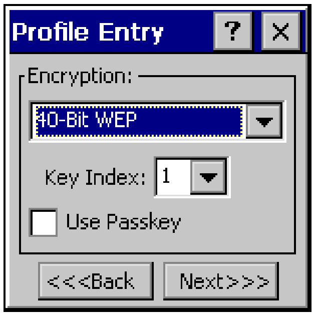
Domain:

Figure 6-22 *Advanced Identity Dialog Box*

Tap **Next**, the **Encryption** dialog box displays.

Encryption

Use the **Encryption** dialog box to select an encryption type. The **Encryption** dialog box only allows encryption types that can be used with the currently selected authentication type. See *Table 6-12* for the encryption types available with each authentication type.



Profile Entry

Encryption: 40-Bit WEP

Key Index: 1

□ Use Passkey

Figure 6-23 *Encryption Dialog Box*

Table 6-11 *Encryption Options*

Encryption	Description
Open	Use the *Open* option as the default setting when no data packet encryption is needed over the network. Selecting this option provides no security for the data being transmitted over the network.
40-Bit WEP	Select 40-Bit WEP for the adapter to use the 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 * within the encryption key fields. If the associated AP is using an optional passkey, the active adapter WLAN profile is required to 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.
128-Bit WEP	Select 128-Bit WEP for the adapter to use the 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 * within the encryption key fields. If the associated AP is using an optional passkey, the active adapter WLAN profile is required to 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.
TKIP	Select this option to use Wireless Protected Access (WPA) via TKIP. Manually enter the shared keys in the passkey field. Tap **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.

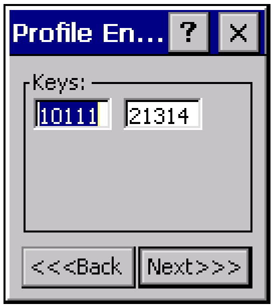
Table 6-12 *Encryption / Authentication Matrix*

	Encryption			
Authentication	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

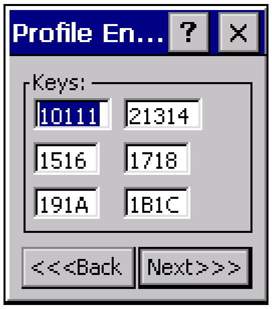
If either **40-Bit WEP** or **128-Bit WEP** is selected the wizard proceeds to the key entry dialog box unless the **Use Passkey** check box was selected in the Encryption Dialog Box (see *Figure 6-23 on page 6-18*). The **Key Entry** dialog box will be shown only if the authentication is set to **None**. To enter the key information:

1. Enter the 40-bit or 128-bit keys into the fields.
2. Tap **Next**.



Keys:
10111 21314

Figure 6-24 *40-Bit WEP Keys Dialog Box*



Keys:
10111 21314
1516 1718
191A 1B1C

Figure 6-25 *128-Bit WEP Keys Dialog Box*

Passkey Dialog

When a user selects **None** as an authentication and **WEP** as an encryption, the user can chose 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 a user selects **None** as an authentication and **TKIP** as an encryption, the user is forced to 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**.

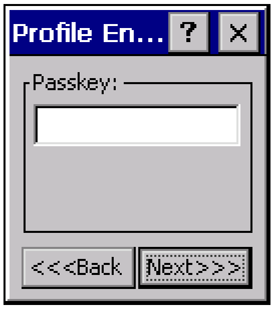
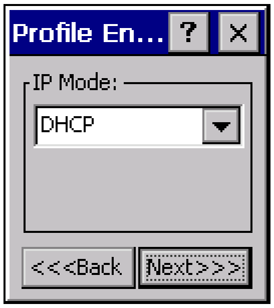


Figure 6-26 *Passkey Dialog Box*

Tap **Next**. The **IP Mode** dialog box displays.

IP Mode

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



IP Mode: DHCP

Figure 6-27 *IP Config Tab (DHCP)*

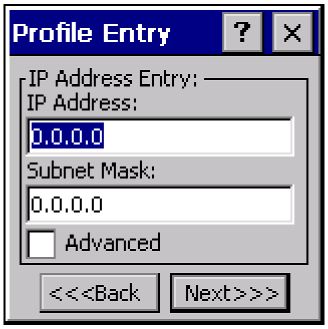
Table 6-13 *IP Mode Options*

Encryption	Description
DHCP	Select **Dynamic Host Configuration Protocol (DHCP)** from the **IP Mode** drop-down list to obtain a leased IP address and network configuration information from a remote server. DHCP is the default setting for the mobile computer 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 used by the mobile computer profile.

Select either **DHCP** or **Static** from the drop-down list and then tap **Next**. If **Static IP** is selected, the **IP Address Entry** dialog box displays. If **DHCP** is selected, the **Transmit Power** dialog box displays.

IP Address Entry

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



Profile Entry

IP Address Entry:

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

□ Advanced

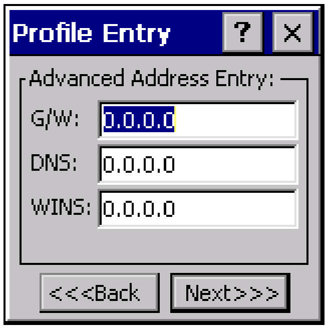
Figure 6-28 *Static IP Address Entry Dialog Box*

Table 6-14 *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 in order to effectively manage routed IP addresses. Having an organization's network divided into subnets allows it to be connected to the Internet with a single shared network address, for example, 255.255.255.0.

Select the **Advanced** check box to enter additional address information.

If the **Advanced** check box is selected then tapping **Next** displays the **Advanced Address Entry** dialog box to enter the Gateway, DNS, and WINS address. If the **Advanced** check box is not selected then tapping **Next** displays the **Transmit Power** dialog box.



Profile Entry

Advanced Address Entry:

G/W: 0.0.0.0

DNS: 0.0.0.0

WINS: 0.0.0.0

Figure 6-29 *Advanced Address Entry Dialog Box*

The IP information that is entered in the profile is only used when the **Enable IP Mgmt** check box is enabled in the **Options** > **System Options** dialog box (*System Options on page 6-38*). When **Enable IP Mgmt** check box is disabled, the IP information in the profile is ignored and the IP information entered in the Microsoft interface applies.

Table 6-15 *IP Config Advanced Address Entry Fields*

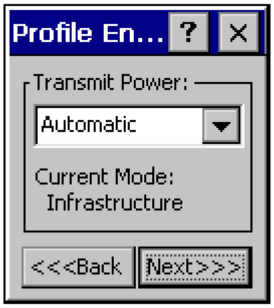
Field	Description
G/W	The default Gateway is a device that is used to forward IP packets to and from a remote destination.
DNS	The Domain Name System (DNS) is a distributed Internet directory service. DNS is used mostly to translate domain names and IP addresses. It is also used to control Internet email delivery. Most Internet service requires 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.

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

Transmit Power

The transmit power can be selected for both Ad-Hoc and Infrastructure network types. The **Transmit Power** drop-down list contains different options for each 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 a coverage area in high traffic areas improves transmission quality by reducing the amount of interference in that coverage area.



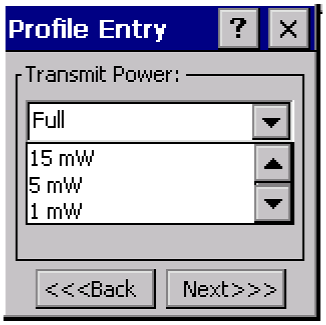
Transmit Power: Automatic

Current Mode: Infrastructure

Figure 6-30 *Transmit Power Dialog Box (Infrastructure Mode)*

Table 6-16 *Transmit Power Dialog Box (Infrastructure Mode)*

Field	Description
Automatic	Select **Automatic** to use the AP power level. **Automatic** is the default mode for mobile computers operating in **Infrastructure** mode.
Power Plus	Select **Power Plus** to set the mobile computer transmission power one level higher than the level set for the AP.


Profile Entry

Transmit Power:

Full

15 mW
5 mW
1 mW

Figure 6-31 *Transmit Power Dialog Box (Ad-Hoc Mode)*

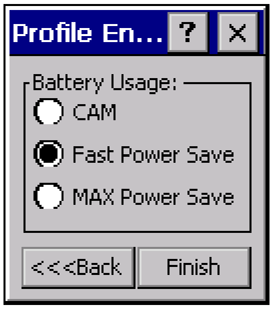
Table 6-17 *Power Transmit Options (Ad-Hoc Mode)*

Field	Description
Full	Select **Maximum** power to set the mobile computer to the highest transmission power level. Select **Maximum** power when operating in highly reflective environments and areas where other devices could be operating nearby. Additionally, use the maximum power level 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 that power level.
15 mW	Select 15 mW, to set the transmit power level to that power level.
5 mW	Select 5 mW to set the transmit power level to that power level.
1 mW	Select **Minimum** power to set the mobile computer to the lowest transmission power level. Use the minimum power level when communicating with other devices in very close proximity. Additionally, select minimum power in instances where little or no radio interference from other devices is anticipated.

Tap **Next** to implement power consumption changes for the mobile computer profile. the **Battery Usage** dialog box displays.

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.



Profile En...

Battery Usage:

○ CAM

● Fast Power Save

○ MAX Power Save

Figure 6-32 *Battery Usage Dialog Box*

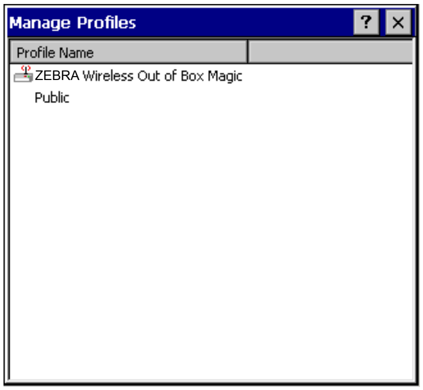
✓ ***NOTE*** Power consumption is also related to the transmit power settings.

Table 6-18 *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 performs in the middle of CAM and MAX Power Save with respect to network performance and battery life. Default.
MAX Power Save	Max Power Save yields the longest battery life while potentially reducing network performance. In networks with minimal latency. Max Power Save will perform just as well as Fast Power Save, but with increased battery savings.

Manage Profiles Application

The **Manage Profiles** window provides a list of user configured wireless profiles. Up to 32 profiles can be defined at any one time. To open the **Manage Profiles** window, tap the **Signal Strength** icon > **Manage Profiles**. The **Manage Profiles** window displays.



Manage Profiles

Profile Name	
ZEBRA Wireless Out of Box Magic	
Public	

Figure 6-33 *Manage Profiles Window*

Icons next to each profile identify the profiles current state.

Table 6-19 *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 currently in use and describes an infrastructure profile not using encryption.
📡🔑	Profile is currently in use and describes an infrastructure profile using encryption.
🖥	Profile is currently in use and describes an ad-hoc profile not using encryption.
🖥🔑	Profile is currently 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. Edit existing profiles by selecting one in the list and then tap-and-hold to display the menu. The menu allows the selected profile to be connected, edited, disabled (enabled) or deleted. (Note: the **Disable** menu item changes to **Enable** if the profile is already disabled.)

A dialog displays to confirm the users desire to delete a profile, if selected.

Changing Profiles

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

Select a profile from the list. Select **Connect** from the pop-up menu to set that profile as the active profile. Once selected, the mobile computer uses the authentication, encryption, ESSID, IP Config and power consumption settings initially configured for that profile.

Editing a Profile

Select a profile from the list. Select **Edit** from the pop-up menu to display the **Profile Wizard** where the ESSID and operating mode can be changed for the profile. Use the wizard to edit the profile power consumption and security parameters*. See Profile Editor Wizard on page 6-6* for procedure on using the wizard.

Creating a New Profile

Create new profiles from the **Manage Profiles** window by performing a tap-and-hold anywhere in this window. A menu with only the **Add** highlighted displays.

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

Deleting a Profile

To delete a profile from the list and select **Delete** from the pop-up menu. A confirmation dialog box appears.

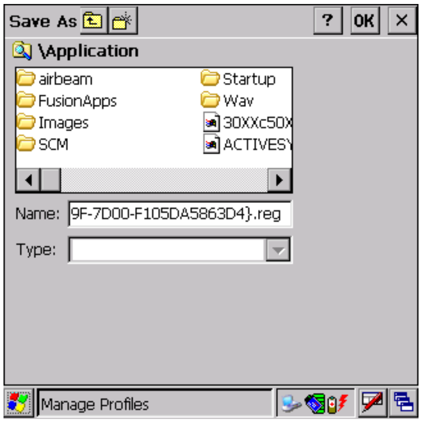
Ordering Profiles

Select a profile from the list and select **Move Up** or **Move Down** from the pop-up to order the profile. If the current profile association is lost, the mobile computer attempts to associate with the first profile in the list and then the next until a new association is achieved.

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

Export a Profile

To export a profile to a registry file, select a profile from the list and select **Export** from the pop-up menu. The **save As** dialog box displays with the **Application** folder and a default name of WCS_PROFILE{*profile GUID*}.reg (Globally Unique Identifier).



Name: 9F-7D00-F105DA5863D4}.reg

Figure 6-34 *Save As Dialog Box*

If required, change the **Name** field and tap **OK**. A confirmation dialog box appears after the export is complete.

Wireless Status Application

The **Wireless Status** application window displays the current wireless connection status and information about the wireless connection.

To open the **Wireless Status** window, tap the **Signal Strength** icon > **Wireless Status**. The **Wireless Status** window displays.

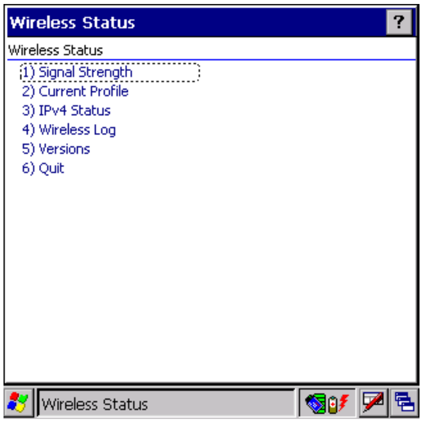


Figure 6-35 *Wireless Status Window*

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

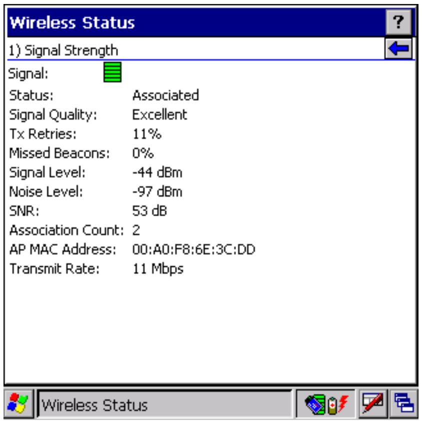
- Signal Strength - provides information about the connection status of the current wireless profile.
- Current Profile - displays basic information about the current profile and connection settings
- IPv4 Status - displays the current IP address, subnet and other IP related information assigned to the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

Option windows contain a back button ⬅ to return to the main **Wireless Status** window.

Signal Strength Window

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

To open the **Signal Status** window, tap **Signal Strength** in the **Wireless Status** window. The **Signal Strength** window displays.


Wireless Status ?

1) Signal Strength

Signal: 🟩

Status: Associated

Signal Quality: Excellent

Tx Retries: 11%

Missed Beacons: 0%

Signal Level: -44 dBm

Noise Level: -97 dBm

SNR: 53 dB

Association Count: 2

AP MAC Address: 00:A0:F8:6E:3C:DD

Transmit Rate: 11 Mbps

Figure 6-36 *Signal Strength Window*

After viewing the **Signal Strength** window, tap the back button to go back to the **Wireless Status** window.

Table 6-20 *Signal Strength Status*

Field	Description
Signal Quality	Displays the Relative Signal Strength Indicator (RSSI) of the signal transmitted between the AP and mobile computer. 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 turned off or there are issues communicating to the radio card.
Status	Indicates if the mobile computer is associated with the AP.
Signal Quality	Displays a text format of the Signal Quality icon. Excellent Signal Very Good Signal Good Signal Fair Signal Poor Signal Out of Range (No Signal).
Tx Retries	Displays a percentage of the number of data packets retransmitted by the mobile computer. The fewer transmit retries, the more efficient the wireless network is.
Missed Beacons	Displays a percentage of the amount of beacons missed by the mobile computer. 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.

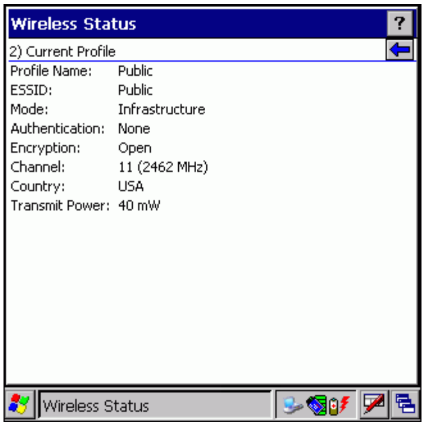
Table 6-20 *Signal Strength Status*

Field	Description
Signal Level	The AP signal level in decibels per milliwatt (dBm).
Noise Level	The background interference (noise) level in decibels per milliwatt (dBm).
SNR	The access point/mobile computer Signal to Noise Ratio (SNR) of signal strength to noise (interference) in decibels per milliwatt (dBm).
Roaming Count	Displays the number of APs that the mobile computer has connect to while roaming.
AP MAC Address	Displays the MAC address of the AP to which the mobile computer is currently connected to.
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, tap **Current Profile** in the **Wireless Status** window. The **Current Profile** window displays.



```
Profile Name:    Public
ESSID:           Public
Mode:            Infrastructure
Authentication:  None
Encryption:      Open
Channel:         11 (2462 MHz)
Country:         USA
Transmit Power:  40 mW
```

Figure 6-37 *Current Profile Window*

Table 6-21 *Current Profile Fields*

Field	Description
Profile Name	Displays the current profile name that the mobile computer is using 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.

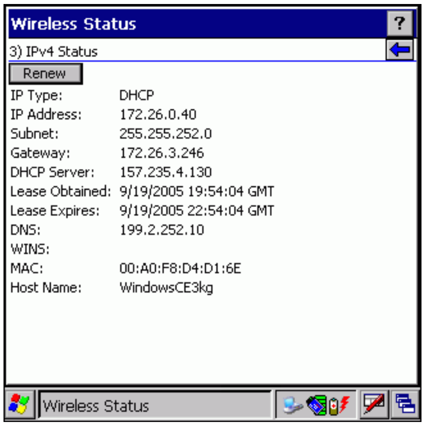
Table 6-21 *Current Profile Fields*

Field	Description
Channel	Displays the current profile channel setting.
Country	Displays the current profile 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 mobile computer. It also allows the address to be renewed if it the profile is currently using DHCP to obtain the IP information. When the user tap **Renew** a full DHCP discover initiates. The **IPv4 Status** window should update automatically when the IP address changes.

To open the **IPv4 Status** window, tap **IPv4 Status** in the **Wireless Status** window. The **IPv4 Status** window displays.



```
IP Type:        DHCP
IP Address:     172.26.0.40
Subnet:         255.255.252.0
Gateway:        172.26.3.246
DHCP Server:    157.235.4.130
Lease Obtained: 9/19/2005 19:54:04 GMT
Lease Expires:  9/19/2005 22:54:04 GMT
DNS:            199.2.252.10
WINS:
MAC:            00:A0:F8:D4:D1:6E
Host Name:      WindowsCE3kg
```

Figure 6-38 *IPv4 Status Window*

Table 6-22 *IPv4 Status Fields*

Field	Description
IP Type	DIsplays the IP type for the current profile, either DHCP or Static. If the current IP type is DHCP, leased IP address and network address data display for the mobile computer. If the current IP type is Static, the values displayed were input manually in the **IP Config** tab on page 6-21.
IP Address	Displays the IP address assigned to the mobile computer. 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 in order to effectively manage routed IP addresses. Having an organization's network divided into subnets allows it to be connected to the Internet with a single shared network address, for example, 255.255.255.0.

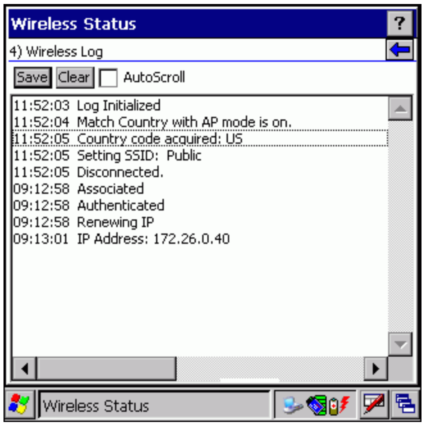
Table 6-22 *IPv4 Status Fields (Continued)*

Field	Description
Gateway	Displays the gateway address. A gateway is a device that is used to forward IP packets to and from a remote destination.
DCHP Server	The Domain Name System (DNS) is a distributed Internet directory service. DNS is used mostly to translate domain names and IP addresses. It is also used to control Internet e-mail delivery. Most Internet service requires 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 the mobile computer is assigned at the factory that uniquely identifies the adapter at the physical layer.
Host Name	Displays the name of the mobile computer.

Wireless Log Window

The **Wireless Log** window displays a log of important recent activity, such as authentication, association, DHCP renewal completion, in time order. Users can choose to save the log to a file or to clear the log (within this instance of the application only). There is also an auto scroll feature to automatically scroll down when new items are added to the log.

To open the **Wireless Log** window, tap **Wireless Log** in the **Wireless Status** window. The **Wireless Log** window displays.



```
11:52:03  Log Initialized
11:52:04  Match Country with AP mode is on.
11:52:05  Country code acquired: US
11:52:05  Setting SSID:  Public
11:52:05  Disconnected.
09:12:58  Associated
09:12:58  Authenticated
09:12:58  Renewing IP
09:13:01  IP Address: 172.26.0.40
```

Figure 6-39 *Wireless Log Window*

Saving a Log

To save a Wireless Log:

1. Tap the **Save** button. The **Save As** dialog box displays.

2. Navigate to the desired folder.
3. In the **Name** filed, enter a file name and then tap **OK**. A text file is saved in the selected folder.

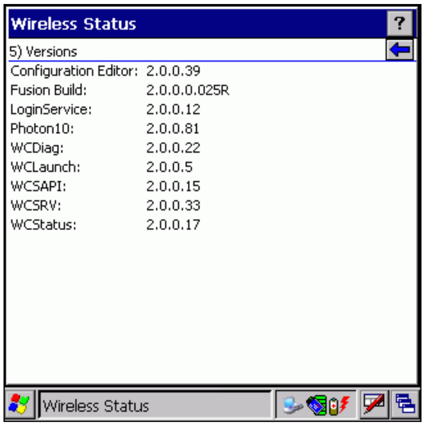
Clear the Log

To clear the log, tap **Clear**.

Versions Window

The **Versions** window displays software, firmware and hardware version numbers. This window only updates each time 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” is displayed if the executable cannot be found at the specified path.

To open the **Versions** window, tap **Versions** in the **Wireless Status** window. The **Versions** window displays.



```
Configuration Editor:  2.0.0.39
Fusion Build:          2.0.0.0.025R
LoginService:          2.0.0.12
Photon10:              2.0.0.81
WCDiag:                2.0.0.22
WCLaunch:              2.0.0.5
WCSAPI:                2.0.0.15
WCSRV:                 2.0.0.33
WCStatus:              2.0.0.17
```

Figure 6-40 *Versions Window*

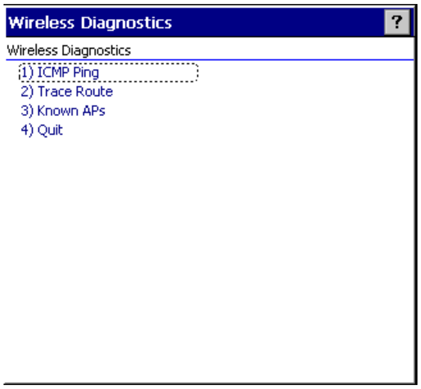
The window displays software version numbers for the following:

- Configuration Editor (Fusion 2.4 and below)
- Fusion Build
- LoginService
- Photon10
- PublicAPI (Fusion 2.5 and above)
- WCConfigEd (Fusion 2.5 and above)
- WCDig
- WCLaunch
- WCSAPI
- WCSRV
- WCStatus.

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, tap the **Signal Strength** icon > **Wireless Diagnostics**. The **Wireless Diagnostics** window displays.



Wireless Diagnostics
1) ICMP Ping
2) Trace Route
3) Known APs
4) Quit

Figure 6-41 *Wireless Diagnostics Window*

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

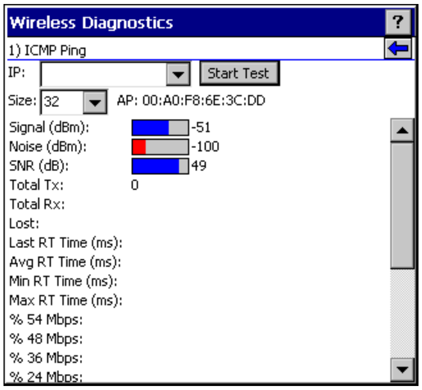
- ICMP Ping - tests the wireless network connection.
- Trace Route - tests a connection at the network layer between the mobile computer and any place on the network.
- Known APs - displays the APs in range using the same ESSID as the mobile computer.
- Quit - Exits the **Wireless Diagnostics** window.

Option windows contain a back button ⬅ to return to the main **Wireless Diagnostics** window.

ICMP Ping Window

The **ICMP Ping** window allows a user to test a connection at the network layer (part of the IP protocol), between the mobile computer and an AP. Ping tests only stop when the user taps the **Stop Test** button, closes the **Wireless Diagnostics** application, or if the mobile computer switches between infrastructure and ad-hoc modes.

To open the **ICMP Ping** window, tap the **ICMP Ping** in the **Wireless Diagnostics** window. The **ICMP Ping** window displays.



IP:
Size: 32
AP: 00:A0:F8:6E:3C:DD
Signal (dBm): -51
Noise (dBm): -100
SNR (dB): 49
Total Tx: 0
Total Rx:
Lost:
Last RT Time (ms):
Avg RT Time (ms):
Min RT Time (ms):
Max RT Time (ms):
% 54 Mbps:
% 48 Mbps:
% 36 Mbps:
% 24 Mbps:

Figure 6-42 *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. From the **Size** drop-down list, select a size value.
3. Tap **Start Test**. 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 are occurring.

The **Trace Route** window allows a user to test a connection at the network layer (part of the IP protocol), between the mobile computer and any place on the network.

To open the **Trace Route** window, tap **Trace Route** in the **Wireless Diagnostics** window. The **Trace Route** window displays.

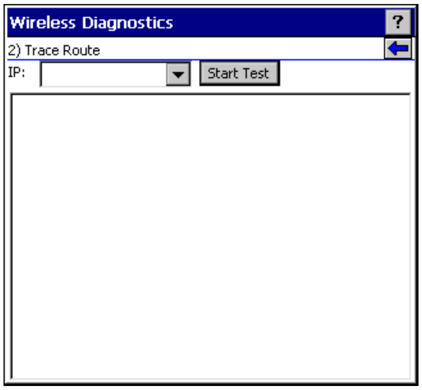


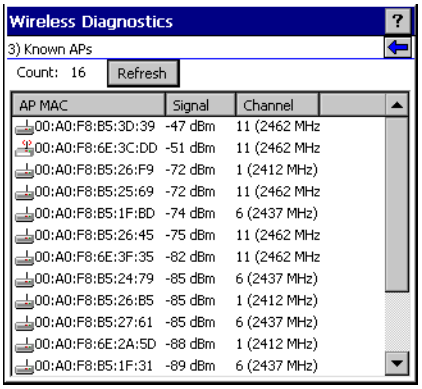
Figure 6-43 *Trace Route Window*

A user can enter an IP address or a DNS Name in the IP combo box, and tap Start Test. The IP combo box should match the same information as shown in the **ICMP Ping** window's IP combo box. When a test is started, the trace route attempts to find all routers between the mobile computer and the destination. The Round Trip Time (RTT) between the mobile computer and each router is shown, and then the total test time is also shown. The total test time may be longer than all RTTs added together because it is not just including time on the network.

Known APs Window

The **Known APs** window displays the APs in range using the same ESSID as the mobile computer. This window only available when in the **Infrastructure** mode.

To open the **Known APs** window, tap **Known APs** in the **Wireless Diagnostics** window. The **Known APs** window displays.



Count: 16

AP MAC	Signal	Channel
00:A0:F8:B5:3D:39	-47 dBm	11 (2462 MHz
00:A0:F8:6E:3C:DD	-51 dBm	11 (2462 MHz
00:A0:F8:B5:26:F9	-72 dBm	1 (2412 MHz)
00:A0:F8:B5:25:69	-72 dBm	11 (2462 MHz
00:A0:F8:B5:1F:BD	-74 dBm	6 (2437 MHz)
00:A0:F8:B5:26:45	-75 dBm	11 (2462 MHz
00:A0:F8:6E:3F:35	-82 dBm	11 (2462 MHz
00:A0:F8:B5:24:79	-85 dBm	6 (2437 MHz)
00:A0:F8:B5:26:B5	-85 dBm	1 (2412 MHz)
00:A0:F8:B5:27:61	-85 dBm	6 (2437 MHz)
00:A0:F8:6E:2A:5D	-88 dBm	1 (2412 MHz)
00:A0:F8:B5:1F:31	-89 dBm	6 (2437 MHz)

Figure 6-44 *Known APs Window*

The icon next to the AP indicates:

The AP is the currently associated access point, and it is set to mandatory.

The AP is the currently associated access point, but it is not set to mandatory.

The mobile computer is not currently associated to this AP, but the AP is set as mandatory.

The mobile computer is not currently associated to this AP, and AP is not set as mandatory.

Tapping and holding the stylus on a specific AP displays a context sensitive menu with the options: **Set Mandatory** and **Set Roaming**.

Selecting the **Set Mandatory** option prohibits the mobile computer from associating with a different AP. The letter **M** displays on top of the icon when the **Set Mandatory** option is selected. The mobile computer connects to the selected AP and never roams until:

- **Set Roaming** is chosen
- The mobile computer roams to a new profile
- The mobile computer is suspended
- The mobile computer resets (warm or cold).

Selecting **Set Roaming** allows the mobile computer to roam to any AP with a better signal. These settings are temporary and never saved to the registry.

Tap **Refresh** to update the list of the APs with the same ESSID. A signal strength value of 32 is the highest possible.

Options

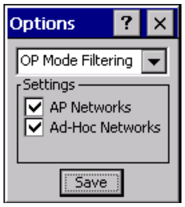
Use the wireless Option dialog box to select various operation settings. The options are saved when **Save** is tapped. If the user taps **X** before saving and an option was changed, a dialog box displays asking the user to close without saving the changes.

The options are:

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

Operating Mode Filtering

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



OP Mode Filtering

☑ AP Networks

☑ Ad-Hoc Networks

Figure 6-45 *OP Mode Filtering Dialog Box*

The default value has both **AP Networks** and **Ad-Hoc Networks** enabled.

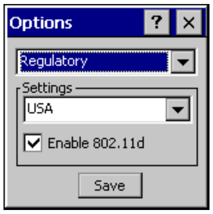
Table 6-23 *OP Mode Filtering Options*

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 6-5*). These are the APs available to the mobile computer profile for association. If this option was previously disabled, refresh the **Available WLAN Networks** window to display the AP networks available to the mobile computer.
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 mobile computer profile for association. If this option was previously disabled, refresh the **Available WLAN Networks** window to display the Ad Hoc networks available to the mobile computer.

Tap **Save** to save the settings or tap **X** to discard any changes.

Regulatory Options

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



Regulatory

Settings

USA

☑ Enable 802.11d

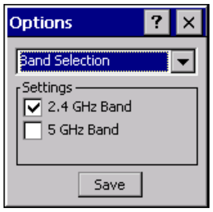
Figure 6-46 *Regulatory Options Dialog Box*

Table 6-24 *Regulatory Options*

Field	Description
Settings	Select the country of use from the drop-down list. In order to connect to a profile, the profile country must match this setting, or the AP country setting if the **Enable 802.11d** check box is selected.
Enable 802.11d	With this check box selected, the WLAN adapter attempts to retrieve the country from APs. Profiles which use **Infrastructure** mode are only able to connect if the country set is the same as the AP country settings or if the profile country setting is set to **Allow Any Country**. Check this box requires that ALL APs be configured to transmit the country information.

Band Selection

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



Band Selection

Settings

☑ 2.4 GHz Band

☐ 5 GHz Band

Figure 6-47 *Band Selection Dialog Box*

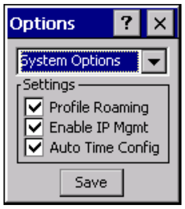
Table 6-25 *Band Selection Options*

Field	Description
2.4GHz Band	With this box checked, the **Find WLANs** application list includes all networks found in the 2.4 GHz band (802.11b and 802.11g).
5GHz Band	With this box checked, the **Find WLANs** application list includes all networks found in the 5 GHz band (802.11a).

Tap **Save** to save the settings or tap **X** to discard any changes.

System Options

Use the system options to set miscellaneous system setting.



☑ Profile Roaming
☑ Enable IP Mgmt
☑ Auto Time Config

Figure 6-48 *System Options Dialog Box*

Table 6-26 *Band Selection Options*

Field	Description
Profile Roaming	Select the **Profile Roaming** check box to configure the mobile computer to roam to the next available WLAN profile when it moves out of range of the current WLAN profile.
Enable IP Mgmt	Select **Enable IP Mgmt** check box to enable the Wireless Companion Services to handle IP Address management. When checked, the Wireless Companion Service configures the IP based on what is configured in the network profile. If unchecked, the Wireless Companion Service does not configure the IP information. For this case, the user must configure the IP in the standard Windows IP dialog screen. Enabled by default.
Auto Time Config	Select **Auto Time Config** check box to enable automatic update of the system time. The device time is updated during network association, based on the time as set in the AP. This proprietary feature is only supported with Zebra infrastructure. Enabled by default.

Change Password Dialog Box

Use the **Change Password** dialog box to require a password before any profile can be edited. This allows system administrators to pre-configure profiles and not allow a user to change the network settings. The user could also use this feature to protect their settings from a guest user. By default, the password is not set.

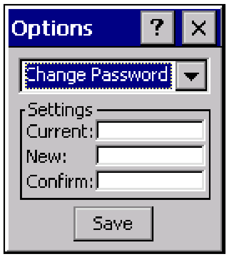


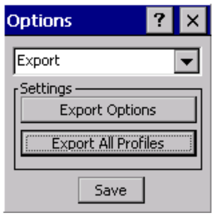
Figure 6-49 *Change Password Window*

1. To create a password for the first time, leave the **Current:** text box empty and enter the new password in the **New:** and **Confirm:** text boxes. Tap **Save**.
2. To change an existing password, enter the current password in the **Current:** text box, enter the new password in the **New:** and **Confirm:** text boxes.Tap **Save.**
3. Delete the password, in this case enter the current password in the **Current:** text box and leave the **New**: and **Confirm:** text boxes empty.

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

Export

Use the **Export** dialog box to export all profiles to a registry file, and to export the options to a registry file. Each of these export functions prompts the user for a filename that is used as the registry file. The “save” dialog box defaults to the application folder, and has a default file name to use. For exporting all profiles, the default filename is: WCS_PROFILES.REG. For exporting the options, the default filename is: WCS_OPTIONS.REG.

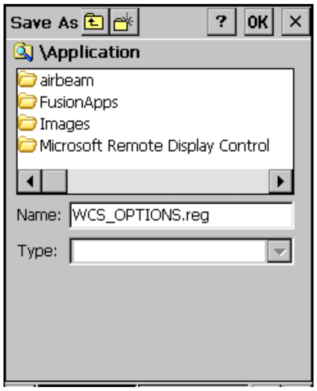


Export

Figure 6-50 *Options - Export Dialog Box*

To export options:

1. Tap **Export Options**. The **Save As** dialog box displays.



Name: WCS_OPTIONS.reg

Type:

Figure 6-51 *Export Options Save As Dialog Box*

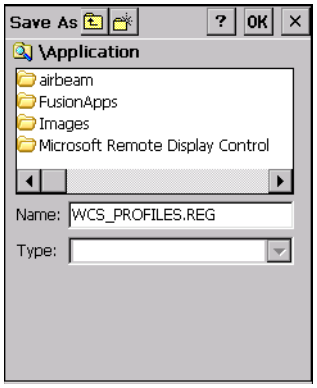
2. The default folder is *\Application\FusionApps\Certs\*.

3. In the Name field, enter a file name.

4. Tap **OK**.

To export all profiles:

1. Tap **Export All Profiles**. The **Save As** dialog box displays.



Name: WCS_PROFILES.REG

Type:

Figure 6-52 *Export All Profiles Save AS Dialog Box*

2. Navigate to the desired folder.
3. In the **Name** field, enter a file name.
4. Tap **OK**.

When **Export All Profiles** is selected the current profile is also saved. This information is used to determine which profile to connect with after a warm boot or cold boot.

Cold Boot Persistence

Exporting options and profiles can be used to provide cold boot persistence. If the exported registry files are saved in the **Application** folder, they are automatically utilized on a cold boot, restoring previous profile and option settings.

Currently, only server certificates can be saved for cold boot persistence. To save server certificates for cold boot persistence, the certificate files must be placed in the folder **Application**. Saving the certificates to this folder causes the certificates to be installed automatically on a cold boot.

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

Registry Settings

Some of the parameters can be modified through a registry key. The registry path is:

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

Table 6-27 *Registry Parameter Settings*

Key	Type	Default	Description
CertificateDirectory	REG_SZ	\\Application	The default directory to find certificates.
EncryptionMask	REG_DWORD	0x0000001F	Defines the encryption types that are currently supported. This is a bitwise mask with each bit corresponding to an encryption type. 1 = Type is supported, 0 = Type is not supported Bit NumberEncryption Type 0None 140-Bit WEP 2128-Bit WEP 3TKIP 4AES (Fusion 2.5 and above only)

Login, Log Off Application

When the user launches the login, log off application, the mobile computer may be in two states; the user may already be logged onto the mobile computer (having already entering credentials through the login box) or the user is not 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 in to the mobile computer, launch the login dialog box to:

- Connect to and re-enable a cancelled profile. To perform this function:
  - Launch the Log On/Off dialog.
  - Select the cancelled profile from the profile list.
  - Login to the profile.

    NOTE: Cancelled profiles can also be re-enabled by using the Profile Editor Wizard and choosing to connect to the cancelled profile. Cancelled profiles are also be re-enabled when a new user logs on.
- Logoff the mobile computer, to prevent another user from accessing the current users network privileges.
- Switch mobile computer users, to quickly logoff the mobile computer and allow another user to log into the mobile computer.

No User Logged In

To access user profiles, when no user is logged in, launch the login dialog box and login.

The dialog displays differently if it is:

- Launched by WCS, when the service is connecting to a new profile that needs credentials
- Launched by WCS, when 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 6-28 *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).
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.

Tapping **OK** sends the credentials though 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 tapped, 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. Tapping **Cancel** closes the Log Off dialog box and the Login dialog box displays.

When the user is logged off, the mobile computer 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, tapping **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 suppressed until a user actively re-enables it or a new user logs onto the mobile computer.

Chapter 7 Staging and Provisioning

Introduction

This chapter describes how to stage devices using Rapid Deployment and provisioning using MSP Agent or AirBEAM Smart.

Staging

Staging is the process of setting up the mobile computer to download packages for provisioning. The mobile computer uses the Rapid Deployment (RD) Client for staging.

✓ ***NOTE*** For Windows CE 5.0 devices:
OEM version 04.22.0001 and lower use MSP 2.X RD Client version 1.9.0.
OEM version 05.26.0000 and higher use MSP 3.X RD Client version 3.28.
OEM version 06.30.0000 and higher use MSP 3.X RD Client version 4.43.

For Windows Mobile 6.1 devices:
OEM version 01.06.0000 uses MSP 3.X RD Client version 4.66.

RD Client Version 1.9.0

The Rapid Deployment (RD) Client version 1.9.0 facilitates software downloads to a mobile computer from a Mobility Services Platform (MSP) Console's FTP server. The MSP Console is a web-based interface to the wireless infrastructure monitoring and management tools provided by the MSP Lite or MSP Enterprise server.

When software packages are transferred to the FTP server, the mobile computer on the wireless network can download them to the mobile computer. The location of software packages are encoded in RD bar codes. When the mobile computer scans a bar code(s), the software package(s) is downloaded from the FTP server to the mobile computer. A single RD bar code can be scanned by multiple mobile computers.

✓ ***NOTE*** For detailed information about the MSP Console, MSP Lite/MSP Enterprise servers and creating RD bar codes, refer to the *MSP Users Guide, p/n* 72E-91844-xx.

The **Rapid Deployment** window displays bar code scan status and provides features for resetting and exiting the application

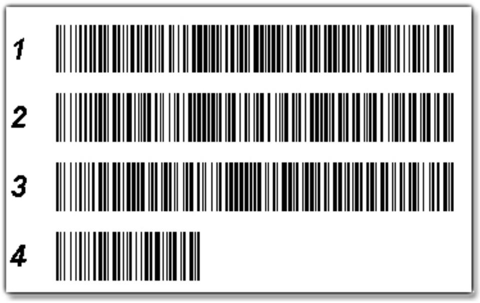
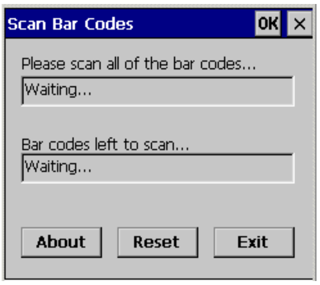


Figure 7-1 *RD Bar Code Printout Sample*

To access the **Rapid Deployment** window tap ⊞ > **Programs** > **Rapid Deployment Client**.



Please scan all of the bar codes...

Waiting...

Bar codes left to scan...

Waiting...

Figure 7-2 *Rapid Deployment Window (Version 1.9.0)*

Table 7-1 *Rapid Deployment Application Descriptions*

Text Box/Button	Description
Please scan all of the bar codes...	Displays the status of a scanned bar code. *Waiting* - indicates the mobile computer is ready to scan a bar code. *OK* - indicates the mobile computer successfully scanned a bar code. (The Indicator LED bar on the mobile computer turns green and a beep sounds). If there are no bar codes left to scan, the **Rapid Deployment Configuring** window displays.
Bar codes left to scan...	Displays a list of any remaining bar codes to scan (1-D bar codes only). When all required bar codes are scanned successfully, the **Rapid Deployment Configuring** window displays.
About	Displays the **Rapid Deployment Client Info** window.
Reset	Removes any previously scanned data.
Exit	Closes the application. A confirmation window displays. Tap **Yes** to exit or **No** to return to the **Rapid Deployment** window. Note: If the application is exited prior to scanning all required bar codes, any scanned data collected up to that point is lost.

Scanning RD Bar Codes

✓ ***NOTE*** Use only a scanner connected to the serial port when scanning bar codes using the RD Client.

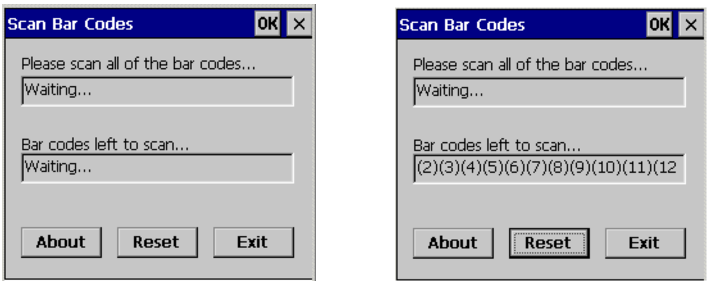
When the mobile computer scans and successfully decodes a single or multiple RD bar codes, the data encoded in the bar code can:

- Reset the mobile computer’s connection profile. A connection profile is a set of Wireless Application parameters that the mobile computer uses to access the wireless network.
- Initiate downloads of one or more software packages from an FTP server to the mobile computer.

✓ ***NOTE*** RD Client version 1.9.0 only recognizes AirBEAM software packages. See *AirBEAM Smart Client on page 7-20* for more information.

To scan an RD bar code:

1. Obtain the appropriate RD bar code(s) from the MSP Administrator.
2. Launch the RD application on the mobile computer. The **Rapid Deployment** window displays.



Scan Bar Codes

Please scan all of the bar codes...

Waiting...

Bar codes left to scan...

Waiting...

Ready to Scan
No Bar Codes Left to Scan

Scan Bar Codes

Please scan all of the bar codes...

Waiting...

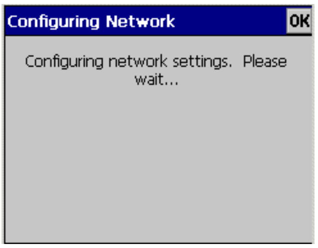
Bar codes left to scan...

(2)(3)(4)(5)(6)(7)(8)(9)(10)(11)(12

Ready to Scan
Bar Codes Left to Scan are Listed

Figure 7-3 *Rapid Deployment Window*

3. Scan the appropriate bar code(s) to complete the configuration and/or download.
   a. A PDF417 bar code (2-D bar code) can contain all download data in a single bar code. In this case, only one bar code may be required to scan.
   b. Multi-part linear bar codes (1-D bar codes) can require scanning several bar codes. Bar codes can be scanned in any order. The text box under **Bar codes left to scan...** shows the remaining bar codes to scan (see *Figure 7-7*).
4. After all appropriate bar codes are scanned successfully, the mobile computer connects to the server and the **Rapid Deployment Configuring** window displays while network settings are configured.



Configuring Network

Configuring network settings. Please wait...

Figure 7-4 *Rapid Deployment Window - Configuring*

✓ ***NOTE*** If the mobile computer cannot connect to the server, it continues to retry until the user cancels (exits) the application. If failure to connect to the server persists, see the MSP Administrator.

5. When configuration is complete:

a. A new Wireless profile is created on the mobile computer from the data encoded in the bar code(s) scanned. See *Chapter 6, Wireless Applications* for more information about wireless profiles.

b. The designated package(s) are downloaded from the FTP server.

RD Client Version 3.28 and above

The RD Client version 3.28 and above enables simple and rapid provisioning of new (out of the box) mobile computers and simplifies the out-of-box provisioning by scanning bar codes or connecting to a profile server. The RD Client acts as a frontend for wireless radio configuration, automating the manual configurations that would normally be required to use these tools.

✓ ***NOTE*** The MSP 3.X Rapid Deployment Client enables staging by scanning staging profiles encoded into staging bar code sheets. It also enables staging to be performed without scanning bar codes through the use of On-Demand Staging.
When using On-Demand Staging, the RD Client pulls staging profiles directly from an On-Demand Profile Server over some form of pre-configured or automatically-configured IP connection.

For detailed information about the MSP 3.X, refer to the *Mobility Services Platform 3.X User's Guide*.

An MSP Administrator uses the MSP Console for the creation of an RD profile that contains all the wireless network and security information (for example, ESSID, WEP Keys, etc.) required to get a mobile computer onto the wireless network. The profile also contains FTP server access information needed to connect to the provisioning MSP and the list of software packages to be provisioned to the mobile computer from the provisioning MSP. The RD profile can then be encoded into an RD bar code sheet and printed from the MSP Console or loaded onto a profile server.

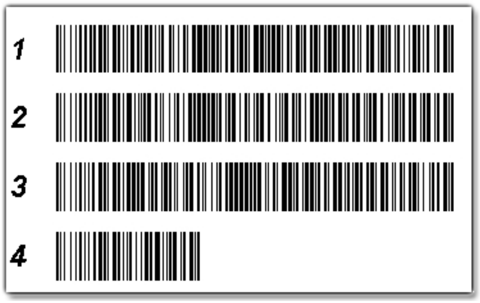


Figure 7-5 *RD Bar Code Printout Sample*

Bar Code Scanning

The **Rapid Deployment** window displays bar code scan status and provides features for resetting and exiting the application.

To access the **Rapid Deployment** window tap ⊞ > **Programs** > **Rapid Deployment Client**.

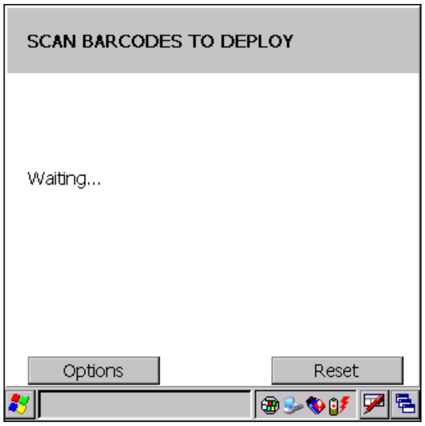
The **Rapid Deployment** window displays bar code scan status and provides features for resetting and exiting the application.

✓ ***NOTE*** Use only a scanner connected to the serial port when scanning bar codes using the RD Client.

To access the **Rapid Deployment** window:

1. Obtain the appropriate RD bar code sheet from the MSP Administrator.

2. Tap > **Programs** > **Rapid Deployment Client**. The **Scan Barcodes To Deploy** window displays.



SCAN BARCODES TO DEPLOY

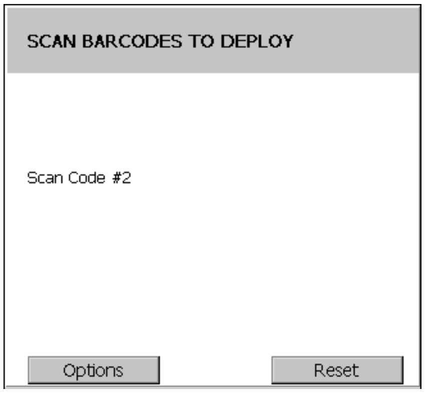
Waiting...

Figure 7-6 *Waiting for Bar Codes*

The RD Client waits for the first bar code scan.

3. Scan the first bar code. The window indicates which bar code to scan next.

✓ ***NOTE*** Multi-part linear bar codes (1-D bar codes) can require scanning several bar codes. Bar codes can be scanned in any order. The display indicate the bar code to scan.

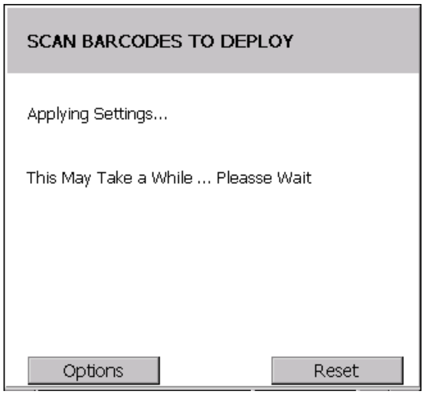


SCAN BARCODES TO DEPLOY

Scan Code #2

Figure 7-7 *Rapid Deployment Window*

4. After all the bar codes are scanned successfully, the mobile computer connects to the server and the **PROCESSING PROFILE** window displays while network settings are configured.



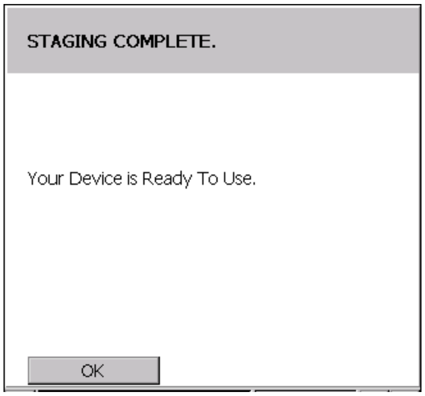
SCAN BARCODES TO DEPLOY

Applying Settings...

This May Take a While ... Pleasse Wait

Figure 7-8 *Rapid Deployment Window - Processing Profile*

5. When staging is complete the **STAGING COMPLETE** window displays.



STAGING COMPLETE.

Your Device is Ready To Use.

Figure 7-9 *Staging Complete Window*

6. Press the left function key to exit the **RD Client**.

On-Demand Staging

The MSP 3.X **RD Client** also enables staging without having to scan bar codes through the use of On-Demand Staging (Electronic Staging).

When using On-Demand Staging, the RD Client pulls staging profiles directly from an On-Demand Profile Server over some form of pre-configured or automatically-configured IP connection. The following types of IP connection modes are currently supported for Electronic Staging:

ActiveSync Connection Mode

This mode uses the IP connection that is established when the mobile computer is directly connected (via a USB cable, serial cable or cradle) to a host computer running ActiveSync. The most common scenario would be where the On-Demand Profile Server is running on the host computer to which the mobile computer is connected via ActiveSync. It would, however, also work with the On-Demand Profile Server running on any other host computer that is on the same subnet as the host computer to which the mobile computer is connected via ActiveSync.

Ethernet Cradle Connection Mode

This mode uses the IP connection that is established when a mobile computer is inserted into an Ethernet cradle that is plugged into the Ethernet LAN. Some mobile computers come ready to use with Ethernet cradles while others require software to be installed and configured before an Ethernet cradle connection can be established. The RD Client does not do anything to install Ethernet cradle software or configure or establish an Ethernet cradle connection, but does use one if it exists. The On-Demand Profile Server must be running on a host computer that is on the same subnet to which the Ethernet cradle is connected.

Already existing IP Connection Mode

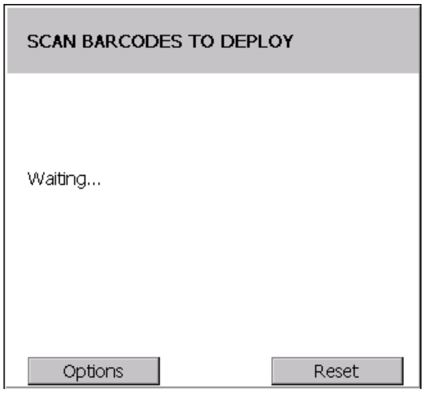
This mode uses any IP connection that is already active on the mobile computer. This could be a direct Ethernet port (if available), or a WLAN connection that was configured and established before the **RD Client** was launched. It could also be any other form of IP connection that might be available on the mobile computer. The **RD Client** does not do anything to configure or establish such connections, but uses them if they exist. The On-Demand Profile Server must be running on a host computer that is on the same subnet that is accessible from the connection.

Well-known WLAN Connection Mode

This mode works only on supported Zebra WLAN adapters. The **RD Client** attempts to configure and establish WLAN IP connections using pre-defined Zebra WLAN settings. If the **RD Client** is able to successfully configure and establish such a connection, and if an On-Demand Profile Server is running on a host computer that is on the same subnet that is accessible from the connection, then Electronic Staging proceeds using that connection.

To perform On-Demand Staging:

1. In the **App Launcher** menu, press the center function key to launch the **RD Client**. The **Scan Barcodes To Deploy** window displays.



SCAN BARCODES TO DEPLOY

Waiting...

Figure 7-10 *Waiting for Bar Codes*

2. Tap **Options**. The **Main Menu** window appears.

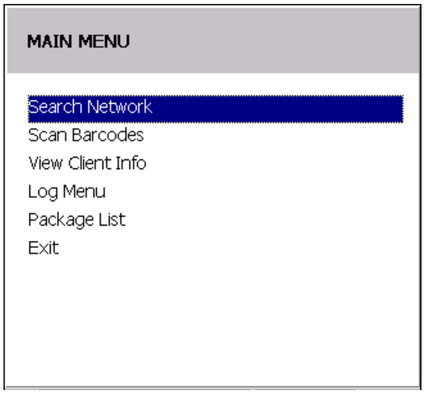
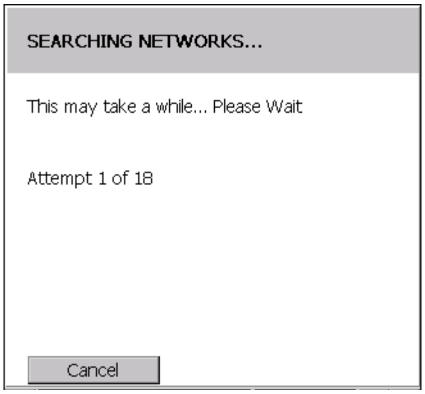


Figure 7-11 *RD Client Main Menu*

3. Select **Search Network**. The **SEARCHING NETWORKS** window appears.
   On RD Clients version 44.3 and above, select **Search Connected Networks** or **Search Unconnected Networks.**
   The **SEARCHING NETWORKS** window appears.



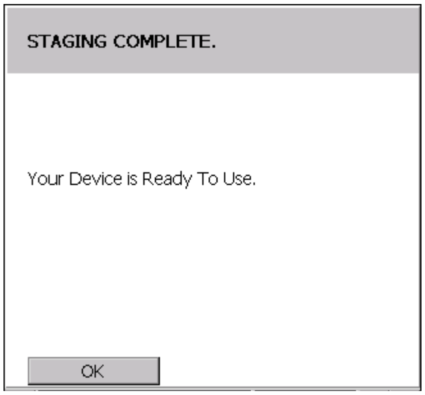
SEARCHING NETWORKS...

This may take a while... Please Wait

Attempt 1 of 18

Figure 7-12 *RD Client Searching for On-Demand Profile Server*

4. When complete, the **STAGING COMPLETE** window displays.



STAGING COMPLETE.

Your Device is Ready To Use.

Figure 7-13 *Staging Complete Window*

Tap OK to exit.

RD Client Main Menu

The RD Client **Main Menu** contains the following options:

- Search Networks. See *On-Demand Staging on page 7-6* for detailed information.
- Scan Barcodes See *Bar Code Scanning on page 7-4* for detailed information.
- View Client Info
- Log Menu
- Package List
- Exit - Closes the RD Client application.

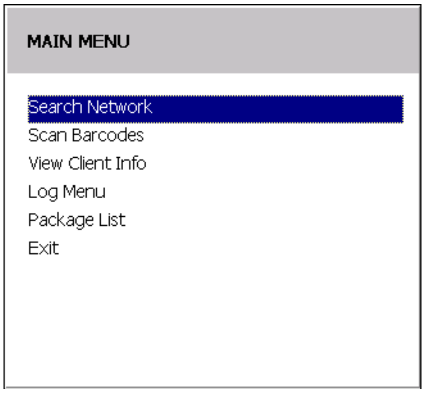


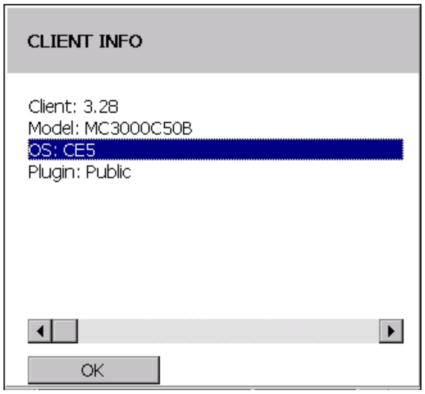
Figure 7-14 *RD Client Main Menu*

Client Info

Use the **Client Info** window to view the following information:

- RD Client version
- Product name
- Operating system type
- Plug-in type.

Tap **View Client Info** option.



Client: 3.28
Model: MC3000C50B
OS: CE5
Plugin: Public

Figure 7-15 *Client Info Window*

Tap **OK** to return to the **Main Menu**.

Log Menu

The **Log Menu** contains the following options:

- View Log
- View Job Log
- Set Log Level
- Set Job Log Level.

Select **Log Menu** option.

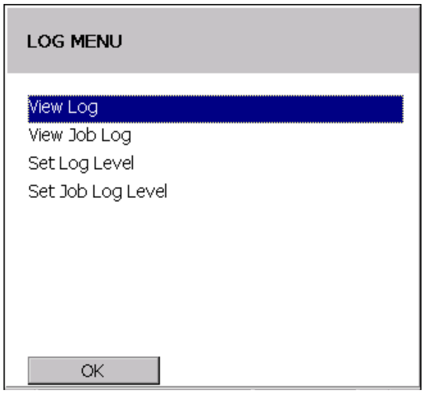


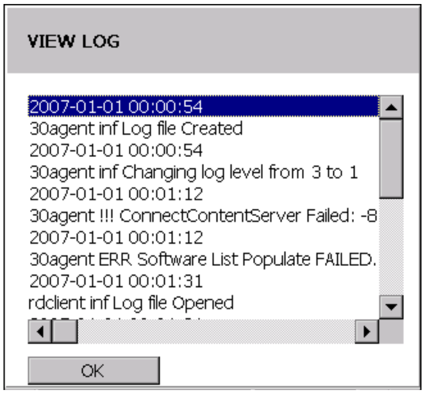
Figure 7-16 *Log Menu Window*

Tap **OK** to return to the **Main Menu**.

View Log

Use the **View Log** option to display a list of events that have occurred.

Select **View Log** option.



```
2007-01-01 00:00:54
30agent inf Log file Created
2007-01-01 00:00:54
30agent inf Changing log level from 3 to 1
2007-01-01 00:01:12
30agent !!! ConnectContentServer Failed: -8
2007-01-01 00:01:12
30agent ERR Software List Populate FAILED.
2007-01-01 00:01:31
rdclient inf Log file Opened
```

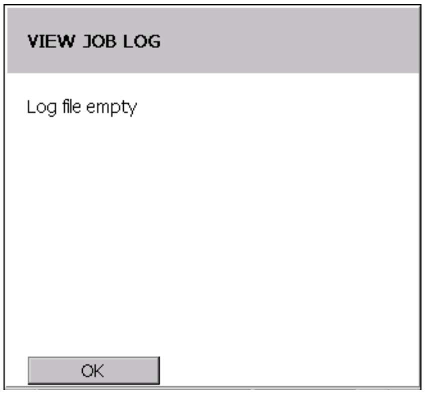
Figure 7-17 *View Log Window*

Tap **OK** to return to the **Log Menu**.

View Job Log

Use the **View Job Log** option to display a list of jobs that have be processed.

Select **View Job Log** option.



VIEW JOB LOG

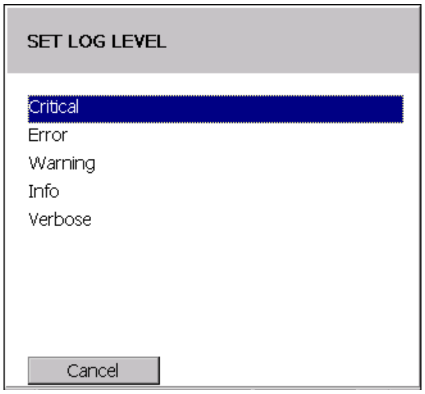
Log file empty

Figure 7-18 *View Job Log Window*

Tap **OK** to return to the **Log Menu**.

Set Log Level

Use the **Set Log Level** option to set the level of the information that appears in the log.



SET LOG LEVEL

Critical
Error
Warning
Info
Verbose

Figure 7-19 *Set Log Level Window*

Select a level option.

Set Job Log Level

Use the **Set Job Log Level** option to set the level of the information that appears in the Job log.

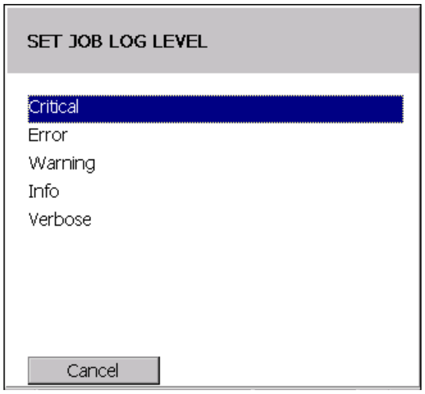


Figure 7-20 *Set Job Log Level Window*

Select a level option.

Package List

Use the **Package List** option to display the packages that have been installed on the mobile computer.

Select the **Package List** option.

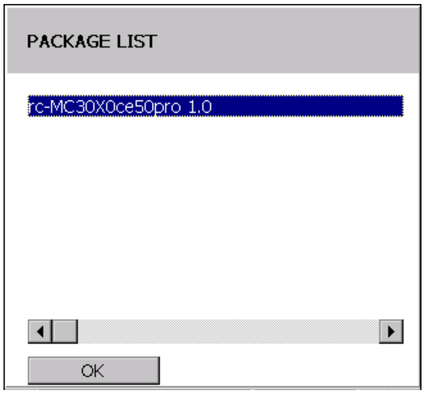


Figure 7-21 *Package List Window*

Tap **OK** to return to the **Main Menu**.

Provisioning

The VC5090 supports two types of provisioning:

- MSP Agent
- AirBEAM Smart Client.

MSP Agent

✓ ***NOTE*** MSP Agent is also known as MSP 3.X Provisioning Client.

The Provisioning Client replaces AirBEAM Client and is responsible for implementing device-side provisioning activities as defined by a policy. A policy is evaluated on the MSP 3.X system and delivered to devices as job documents via relay servers.

The MSP 3.X Provisioning Client is 100% backward compatible to prior versions of the AirBEAM Client. Existing AirBEAM Smart users can use the MSP 3.X Provisioning Client as a 100% backward compatible replacement for prior versions of AirBEAM client, when used in Classic AirBEAM mode with existing FTP servers.

Existing MSP 2.X users can use the new Provisioning Client as a 100% backward compatible replacement for previous versions of AirBEAM Client, when used in Level 2 Agent and Level 3 Agent modes with existing MSP 2.X Appliances.

For more detailed information on MSP Agent (Provisioning Client), refer to the *MSP 3.X User's Guide* (p/n 72E-100158-xx).

MSP Agent Main Menu

The MSP Agent **Main Menu** contains the following options:

- Monitoring Processing
- Force Check-In
- Package List
- View Client info
- Log Menu
- Hide UI
- Exit - exits the MSP Agent application.

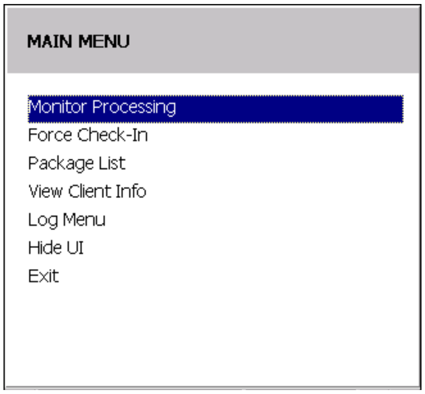
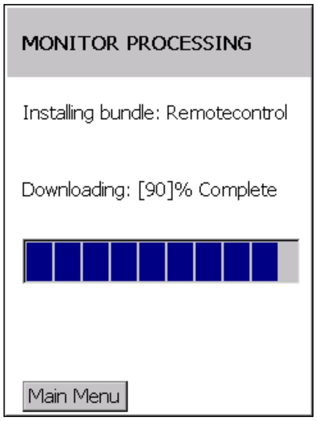


Figure 7-22 *MSP Agent Main Menu*

Monitor Processing

Use the **Monitor Processing** option to view the status of packages being processed.

Select the **Monitor Processing** option.



Installing bundle: Remotecontrol

Downloading: [90]% Complete

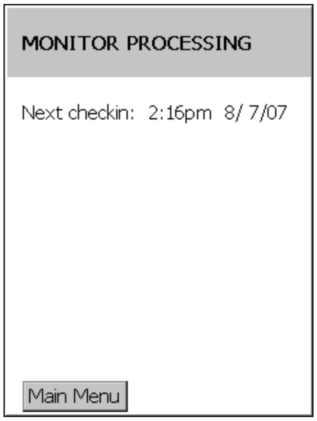
Figure 7-23 *Monitor Processing Window*

Tap **OK** to return to the **Main Menu**.

Force Check-In

Use the **Force Check-In** option to check instantly for pending package downloads instead of waiting for the next automatic check that the client performs.

Select the **Force Check-In** option.



MONITOR PROCESSING

Next checkin: 2:16pm 8/ 7/07

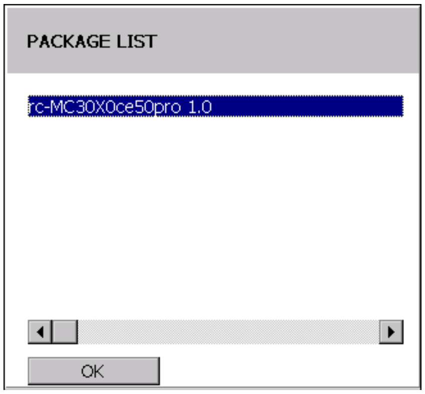
Figure 7-24 *Force Check-in Window*

Tap **OK** to return to the **Main Menu**.

Package List

Use the **Package List** option to display the packages that have been installed on the mobile computer.

Select the **Package List** option.



PACKAGE LIST

rc-MC30X0ce50pro 1.0

Figure 7-25 *Package List Window*

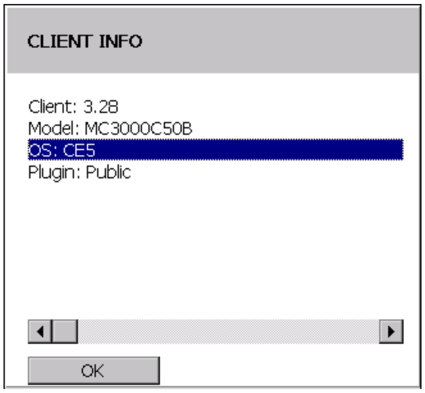
Tap **OK** to return to the **Main Menu**.

Client Info

Use the **Client Info** window to view the following information:

- RD Client version
- Product name
- Operating system type
- Plug-in type.

Select **View Client Info** option.



Client: 3.28
Model: MC3000C50B
OS: CE5
Plugin: Public

Figure 7-26 *Client Info Window*

Tap **OK** to return to the **Main Menu**.

Log Menu

The **Log Menu** contains the following options:

- View Log
- View Job Log
- Set Log Level
- Set Job Log Level.

Select **Log Menu** option.

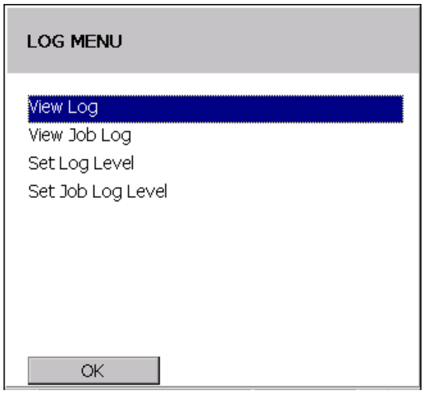


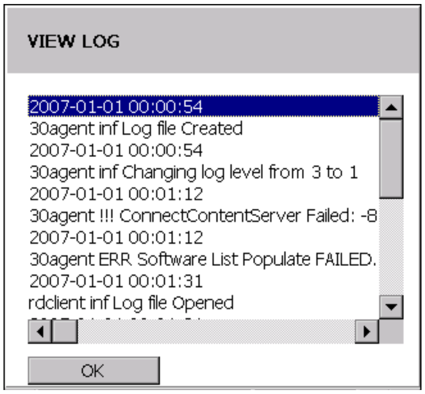
Figure 7-27 *Log Menu Window*

Tap **OK** to return to the **Main Menu**.

View Log

Use the **View Log** option to display a list of events that have occurred.

Select **View Log** option.



```
2007-01-01 00:00:54
30agent inf Log file Created
2007-01-01 00:00:54
30agent inf Changing log level from 3 to 1
2007-01-01 00:01:12
30agent !!! ConnectContentServer Failed: -8
2007-01-01 00:01:12
30agent ERR Software List Populate FAILED.
2007-01-01 00:01:31
rdclient inf Log file Opened
```

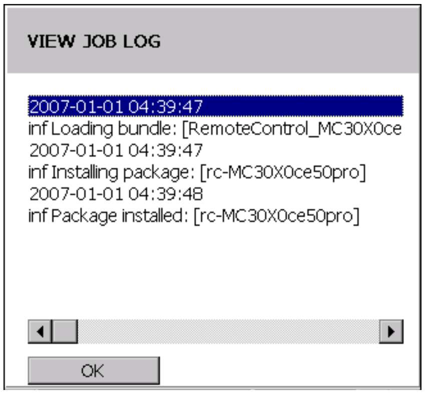
Figure 7-28 *View Log Window*

Tap **OK** to return to the **Log Menu**.

View Job Log

Use the **View Job Log** option to display a list of jobs that have be processed.

Select **View Job Log** option.



```
2007-01-01 04:39:47
inf Loading bundle: [RemoteControl_MC30X0ce
2007-01-01 04:39:47
inf Installing package: [rc-MC30X0ce50pro]
2007-01-01 04:39:48
inf Package installed: [rc-MC30X0ce50pro]
```

Figure 7-29 *View Job Log Window*

Press the left function key to return to the **Log Menu**.

Set Log Level

Use the **Set Log Level** option to set the level of the information that appears in the log.

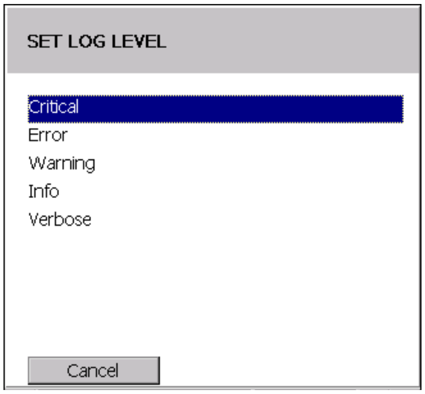


Figure 7-30 *Set Log Level Window*

Select a level option.

Set Job Log Level

Use the **Set Job Log Level** option to set the level of the information that appears in the Job log.

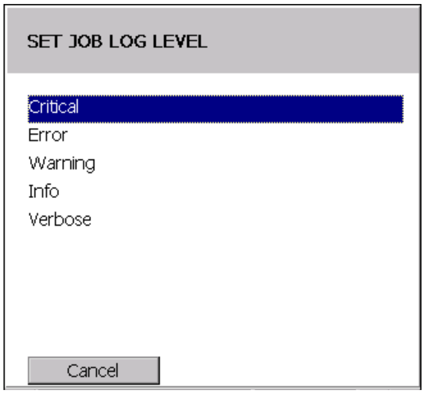


Figure 7-31 *Set Job Log Level Window*

Select a level option.

Hide UI

Use the **Hide UI** option to minimize the MSP Agent application. The MSP Agent application runs in the background while minimized.

To un-hide the application, select the **MSP Agent** icon in the task tray and select the **UnHide UI** menu item.

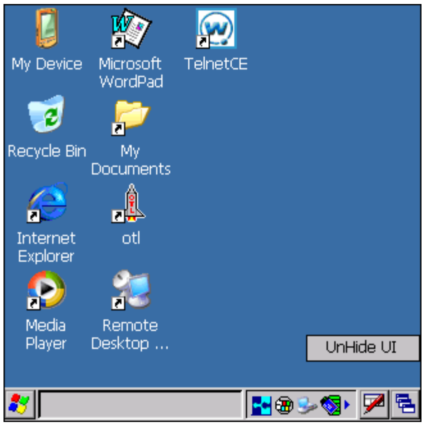


Figure 7-32 *UnHide UI Selection*

AirBEAM Smart Client

The AirBEAM Smart product allows specially designed software packages to be transferred between a host server and a mobile computer. Before transfer, AirBEAM Smart checks and compares package version, so that only updated packages are loaded.

AirBEAM Smart resides on the mobile computer and allows it to request, download and install software, as well as to upload files and status data. Both download and upload of files can be accomplished in a single communications session. The ability to transfer software over a wireless network can greatly reduce the logistical efforts of client software management.

In an AirBEAM Smart system, a network-accessible host server acts as the storage point for the software transfer. The AirBEAM Smart Client uses the industry standard FTP or TFTP file transfer protocols to check the host system for updates and, if necessary, to transfer updated software.

✓ ***NOTE*** For more detailed information about AirBEAM Smart, refer to the AirBEAM® Smart Windows® CE Client Product Reference Guide (p/n 72-63060-xx).

AirBEAM Package Builder

In a typical distributed AirBEAM system, software to be transferred is organized into packages. In general, an AirBEAM package is simply a set of files that are assigned attributes both as an entire package and as individual component files. The package is assigned a version number and the transfer occurs when an updated version is available.

An AirBEAM package can optionally contain developer-specified logic to be used to install the package. Installation logic is typically used to update client device flash images or radio firmware. Examples of common AirBEAM packages would include packages for custom client application software, radio firmware and AirBEAM Smart Client software.

Once these packages are built, they are installed on the host server for retrieval by the mobile computer. The AirBEAM Package Builder is a utility used to define, generate and install AirBEAM packages to a server. The packages are then loaded from the server onto a client device equipped with an AirBEAM Smart Client executable.

For detailed instructions on how to define, generate and install AirBEAM packages to the server, refer to the *AirBEAM Package Builder Product Reference Guide*, p/n 72-55769-xx.

AirBEAM Smart Client

The AirBEAM Smart Client is installed on the mobile computer. It is configured with the server access information, the names of the packages to be downloaded and other controlling parameters. When the AirBEAM Smart Client is launched, the device connects to the specified FTP server and checks the packages it is configured to look for. If the package version was updated, the client requests the transfer.

AirBEAM License

The AirBEAM Smart Client is a licensed software product. The AirBEAM Smart Client's version synchronization functionality is enabled through a license key file that is stored on the mobile computer. The license key file can be built into AirBEAM Smart Client's image, or downloaded in a special AirBEAM package.

The AirBEAM license key file contains a unique key and a customer specific banner that is displayed when the AirBEAM Smart Client version synchronization logic is invoked.

Configuring the AirBEAM Smart Client

1. Connect the mobile computer to a host computer using the Development Cable.

2. Connect to the mobile computer using Remote Desktop. See

3. Select **Start** > **Programs** > **AirBEAM Smart Client**. The **AirBEAM Smart CE** window appears.

4. Select **File** > **Configure**. The **AirBEAM** configuration window appears.

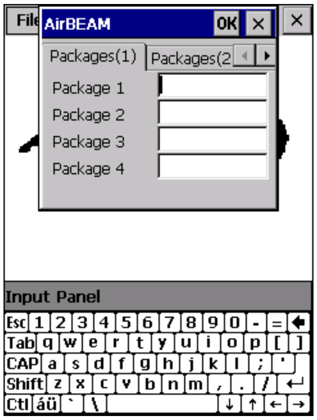


Figure 7-33 *AirBEAM Configuration Window*

The configuration window is used to view and edit AirBEAM Smart Client configurations. This dialog box has seven tabs that you can modify - Packages(1), Packages(2), Server, Misc(1), Misc(2), Misc(3) and Misc(4).

Packages(1) Tab

Use this tab to specify the package name of the first four of eight packages that are to be loaded during the AirBEAM synchronization process. The specified package name must correspond to a package that is available on the specified package server.

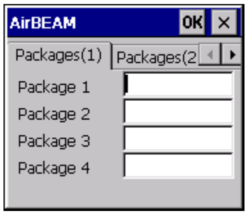


Figure 7-34 *Package (1) Tab*

Table 7-2 *Package (1) Tab Descriptions*

Field	Description
Package 1	Package name of the first of eight packages. This is an optional field.
Package 2	Package name of the second of eight packages. This is an optional field.
Package 3	Package name of the third of eight packages. This is an optional field.
Package 4	Package name of the fourth of eight packages. This is an optional field.

✓ ***NOTE*** No inadvertent trailing spaces should be entered on the Packages(1) tab. Information entered in these fields are case and space sensitive.

Packages(2) Tab

Use this tab to specify the package name of the last four of eight packages that are to be loaded during the AirBEAM synchronization process. The specified package name must correspond to a package that is available on the specified package server.

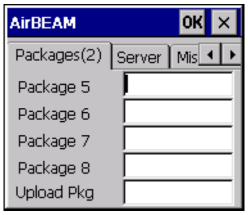


Figure 7-35 *Package (2) Tab*

Table 7-3 *Package (2) Tab Descriptions*

Field	Description
Package 5	Package name of the fifth of eight packages. This is an optional field.
Package 6	Package name of the sixth of eight packages. This is an optional field.
Package 7	Package name of the seventh of eight packages. This is an optional field.
Package 8	Package name of the eighth of eight packages. This is an optional field.
Upload Pkg	Package name of a package that is to be processed for “upload files” during the AirBEAM synchronization process. The specified package name must correspond to a package that is available on the specified package server. This is an optional field.

NOTE No inadvertent trailing spaces should be entered on the Packages(2) tab. Information entered in these fields are case and space sensitive.

Server Tab

Use this tab to specify the configurations of the server to which the client connects during the package synchronization process.

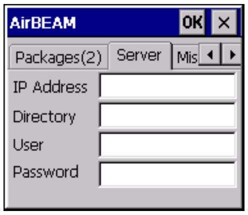


Figure 7-36 *Server Tab*

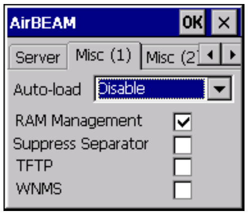
Table 7-4 *Server Tab Descriptions*

Field	Description
IP Address	The IP Address of the server. It may be a host name or a dot notation format.
Directory	The directory on the server that contains the AirBEAM package definition files. All AirBEAM package definition files are retrieved from this directory during the package synchronization process.
User	The FTP user name that is used during the login phase of the package synchronization process.
Password	The FTP password that corresponds to the FTP user specified in the **User** field. The specified password is used during the login phase of the package synchronization process.

NOTE No inadvertent trailing spaces should be entered on the Server tab. Information entered in these fields are case and space sensitive.

Misc(1) Tab

Use this tab to configure various miscellaneous features.



Auto-load Disable

RAM Management ☑
Suppress Separator □
TFTP □
WNMS □

Figure 7-37 *Misc (1) Tab*

Table 7-5 *Misc(1) Tab Descriptions*

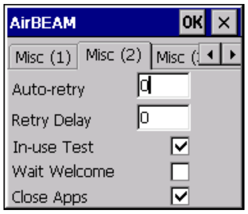
Field	Description
Auto-load	This drop-down list is used to specify how the AirBEAM Smart Client is to be invoked automatically when the client device is rebooted. The selections are: **Disable**: the AirBEAM Smart Client is not invoked automatically during the boot sequence. **Interactive**: the AirBEAM Smart Client is invoked automatically during the boot sequence. The package synchronization process is started automatically. The *Synchronization Dialog* box appears and the user is required to press the **OK** button when the process is complete. **Non-interactive**: the AirBEAM Smart Client is invoked automatically during the boot sequence. The package synchronization process is started automatically. The *Synchronization Dialog* box is displayed, but the user is not required to select **OK** when the process is complete. The *Synchronization Dialog* box terminates automatically. **Background**: the AirBEAM Smart Client is invoked automatically during the boot sequence. The package synchronization process is started automatically. Nothing is displayed while the synchronization process is occurring.

Table 7-5 *Misc(1) Tab Descriptions (Continued)*

Field	Description
RAM Management	This check box specifies whether the automatic RAM management is enabled during the package synchronization process. If enabled, RAM management logic is invoked when there is not enough free disk space to download a package. The RAM management logic attempts to remove any discardable AirBEAM packages resident on the client.
Suppress Separator	This check box specifies whether the automatic insertion of a file path separator character should be suppressed when the client generated server package definition file names. When enabled, the parameter also disables the appending of .apd to the package. This feature is useful for AS/400 systems, in which the file path separator character is a period. When this feature is enabled, the server directory (Directory) and package name (Package 1, Package 2, Package 3 and Package 4) are appended “as is” when building the name for the server package definition file. When this feature is disabled, a standard file path separator is used to separate the server directory (Directory) and package name (Package 1, Package 2, Package 3 and Package 4) when building the name for the server package definition file. In addition, an .apd extension is appended automatically.
TFTP	This check box specifies whether the TFTP protocol is to be used to download files. By default, the AirBEAM Smart Client uses the FTP protocol.
WNMS	This check box specifies whether the AirBEAM Smart Client uploads a WNMS information file at the end of each version synchronization.

Misc(2) Tab

This tab is used to configure various miscellaneous features.



Auto-retry 0
Retry Delay 0
In-use Test ☑
Wait Welcome ☐
Close Apps ☑

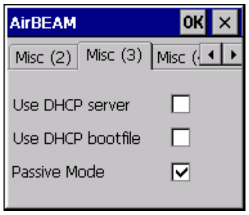
Figure 7-38 *Misc (2) Tab*

Table 7-6 *Misc(2) Tab Descriptions*

Field	Description
Auto-retry	This field is used to specify whether the AirBEAM Smart Client automatically retries if there is a failure during the synchronization process. If this feature is enabled, the AirBEAM Smart Client displays a popup dialog indicating the attempt of a retry. The popup dialog is displayed for the number of seconds specified in the *Retry Delay* field. The valid values for this field are: **-1**: the AirBEAM Smart Client automatically retries indefinitely. **0**: the AirBEAM Smart Client does not automatically retry. **-0**: the AirBEAM Smart Client automatically retries up to the number of times specified.
Retry Delay	This field specifies the amount of time, in seconds, that the AirBEAM Smart Client delays before automatically retrying after a synchronization failure.
In-use Test	This check box specifies whether the AirBEAM Smart Client tests to determine if a file is in-use before downloading. If the *In-use Test* feature is enabled, the AirBEAM Smart Client downloads a temporary copy of any files that are in-use. If any temporary in-use files are downloaded the AirBEAM Smart Client automatically resets the client to complete the copy of the in-use files. If the *In-use Test* feature is disabled, the synchronization process fails (-813) if any download files are in-use.
Wait Welcome	This check box specifies whether the AirBEAM Smart Client waits for the WELCOME windows to be completed before automatically launching the synchronization process after a reset.
Close Apps	This check box specifies whether the AirBEAM Smart Client automatically attempts to close non-system applications prior to resetting the mobile unit. If enabled the AirBEAM Smart Client sends a WM_CLOSE message to all non-system applications before resetting the mobile unit. This feature offers applications the opportunity to prepare (i.e. close open files) for the pending reset.

Misc(3) Tab

Use this tab to configure various miscellaneous features.



Use DHCP server □
Use DHCP bootfile □
Passive Mode ☑

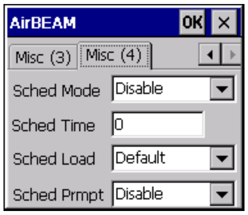
Figure 7-39 *Misc (3) Tab*

Table 7-7 *Misc (3) Tab Descriptions*

Field	Description
Use DHCP server	This check box control specifies whether the AirBEAM Smart Client uses the DHCP response option 66 to specify the *IP address* of the FTP/TFTP server. If enabled, special RF network registry settings are required to force the DHCP server to return the “TFTP server name” field (option 66). The special RF network registry settings are included, but commented out, in the radio network registry initialization files (essid_xxxx_yy.reg).
Use DHCP bootfile	This check box control specifies whether the AirBEAM Smart Client uses the DHCP response option 67 to specify the *Package* and *Package 1* parameters. If enabled, special RF network registry settings are required to force the DHCP server to return the “Bootfile name” field (option 67). The special RF network registry settings are included, but commented out, in the radio network registry initialization files (essid_xxxx_yy.reg).

Misc(4) Tab

Use this tab to configure various miscellaneous features.



Sched Mode: Disable
Sched Time: 0
Sched Load: Default
Sched Prmpt: Disable

Figure 7-40 *Misc (4) Tab*

Table 7-8 *Misc (4) Tab Descriptions*

Field	Description
Sched Mode	Specifies whether (and how) the scheduled mode is enabled. If enabled, schedule mode causes the AirBEAM synchronization process to occur periodically. The selections are: **Disable** - The schedule mode is disabled. **Fixed time** - The schedule mode is enabled. The AirBEAM synchronization will be launched once per day at the time specified in the Sched Time setting. The synchronization will be launched every day Sched Time minutes past midnight. **Fixed period** - The schedule mode is enabled. The AirBEAM synchronization will be launched at a period by the Sched Time setting. The synchronization will be launched every Sched Time minutes.
Sched Time	This edit control specifies, in minutes, the period for the schedule mode. The Sched Mode setting specifies how the Sched Time value is used.

Table 7-8 *Misc (4) Tab Descriptions (Continued)*

Field	Description
Sched Load	This drop-down menu specifies the load mode to be used for scheduled synchronization, if enabled. The selections are: **Default** - Specifies that the load mode specified in the Auto-load setting is to be used for scheduled synchronization sessions. **Interactive** - The Synchronization Dialog displays when a scheduled synchronization session occurs. The user is required to press the OK button to dismiss the dialog. **Non-interactive** - The Synchronization Dialog displays when a scheduled synchronization session occurs. The dialog is automatically dismissed when the synchronization is complete, unless an error occurs. If an error occurs the user is required to press the OK button to dismiss the dialog. **Background** - Nothing is displayed when the scheduled synchronization sessions occur.
Sched Prompt	Specifies whether the AirBEAM client prompts the user when updates are available in schedule mode. The settings are: **Disable** - Updated packages are automatically downloaded. The user is not prompted. **Alert** - Updated packages are not automatically downloaded. The user is prompted to warm boot the device to initiate the package downloads. **Launch** - Updated packages are not automatically downloaded. The user is prompted to start the package download. The user can defer the package download by responding no to the prompt. The MAXNOPRESS registry setting can be used to limit the number of times the user can defer the update. **Confirm** - Updated packages are not automatically downloaded. This value behaves the same as the Launch value, except that the user is required to confirm an additional prompt before the download starts.

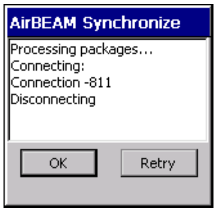
Synchronizing with the Server

When the synchronization process is initiated, the AirBEAM Smart Client attempts to open an FTP session using the AirBEAM Smart Client configuration. Once connected, the client processes the specified packages. Packages are loaded only if the server version of a given package is different from the version loaded on the client. Once the upload process is complete, the AirBEAM Smart Client closes the FTP session with the server.

The AirBEAM Smart Client can launch an FTP session with the server either manually, when initiated by the user, or automatically.

Manual Synchronization

1. Configure the AirBEAM Smart Client. See *Configuring the AirBEAM Smart Client on page 7-20*.
2. From the main *AirBEAM CE* window, press **ALT - ALT** and select **Synchronize**.
3. Once connected, the AirBEAM Synchronize window appears.



```
Processing packages...
Connecting:
Connection -811
Disconnecting
```

Figure 7-41 *AirBEAM Synchronize Window*

- The **Status List** displays status messages that indicate the progress of the synchronization process.
- Press **ENTER** to return to the Main Menu. This button remains inactive until the synchronization process is complete.
- Select **Retry** and press **ENTER** to restart the synchronization process. This button is activated only if there is an error during the synchronization process.

Automatic Synchronization

The AirBEAM Smart Client can be configured to launch automatically using the Misc(1) Preference tab (see *Misc(1) Tab on page 7-23*). When setting automatic synchronization, use the Auto-load drop-down list to specify how the AirBEAM Smart Client should be invoked automatically when the client device is rebooted. See *Misc(1) Tab on page 7-23* for instructions on enabling Auto Sync.

Chapter 8 Maintenance & Troubleshooting

Introduction

This chapter includes instructions on cleaning and storing the mobile computer, and provides troubleshooting solutions for potential problems during mobile computer operation.

Maintaining the Mobile Computer

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

- Do not scratch the screen of the mobile computer. When working with the mobile computer, use the supplied stylus or plastic-tipped pens intended for use with a touch-sensitive screen. Never use a pen or pencil or other sharp object on the surface of the mobile computer screen.
- Although the mobile computer is water and dust resistant, do not expose it to rain or moisture for an extended period of time. In general, treat the mobile computer as a pocket calculator or other small electronic instrument.
- The touch-sensitive screen of the mobile computer is glass. Do not to drop the mobile computer or subject it to strong impact.
- Protect the mobile computer from temperature extremes. Do not leave it on the dashboard of a car on a hot day, and keep it away from heat sources.
- Do not store or use the mobile computer in any location that is extremely dusty, damp, or wet.
- Use a soft lens cloth to clean the mobile computer. If the surface of the mobile computer screen becomes soiled, clean it with a soft cloth moistened with a diluted window-cleaning solution.

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.
- Do not use incompatible batteries and chargers. If you have any questions about the compatibility of a battery or a charger, contact Zebra support. See *Service Information on page xvi* for contact information.

- Do not crush, puncture, or place a high degree of pressure on the battery.
- Severe impact from dropping any battery-operated device on a hard surface could cause the battery to overheat.
- 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.
- Do not dispose of batteries in fire.
- If you suspect damage to your equipment or battery, contact Zebra support to arrange for inspection. See *Service Information on page xvi* for contact information.

Troubleshooting

Mobile Computer

Table 8-1 Troubleshooting the Mobile Computer

Problem	Cause	Solution
Mobile computer does not turn on.	Main battery not charged.	Charge or replace the main battery in the mobile computer.
	Main battery not installed properly.	Ensure the battery is installed properly. For more information see, *Install Main Battery on page 1-6*.
	System crash.	Perform a warm boot. If the mobile computer still does not turn on, perform a cold boot. For more information see, *Resetting the Mobile Computer on page 1-11*.
Battery did not charge.	Battery failed.	Replace battery. If the mobile computer still does not operate, try a warm boot, then a cold boot. For more information see, *Resetting the Mobile Computer on page 1-11*.
	Mobile computer removed from cradle while battery was charging.	Insert mobile computer in cradle and begin charging. The Standard Battery requires up to four hours to recharge fully and the Extended Life Battery requires up to six hours to recharge fully.
	Extreme battery temperature.	Battery does not charge if ambient temperature is below 32°F (0°C) or above 104°F (40°C).
Cannot see characters on screen.	Mobile computer not powered on.	Press the **Power** button.

Table 8-1 Troubleshooting the Mobile Computer (Continued)

Problem	Cause	Solution
During data communication, no data was transmitted, or transmitted data was incomplete.	Mobile computer removed from cradle or unplugged from host computer during communication.	Replace the mobile computer in the cradle, or reattach the cable and re-transmit.
	Incorrect cable configuration.	See *Chapter 2, Accessories* for cable configurations.
	Communication software was incorrectly installed or configured.	Perform communication setup as described in *Communication Setup on page 2-30.*
Mobile computer does not emit sound.	Volume setting is low or turned off.	Mobile computer may be a beeper only configuration or incorrect setting is programmed into device.
Mobile computer turns itself off.	Mobile computer is inactive.	The mobile computer turns off after a period of inactivity. This period can be set from one to five minutes, in one-minute intervals.
	Battery is depleted.	Recharge or replace the battery.
	Battery is not inserted properly.	Insert the battery properly. For more information see, *Install Main Battery on page 1-6*.
Tapping the window buttons or icons does not activate the corresponding feature.	Touch screen not calibrated correctly.	Re-calibrate the screen. From the mobile computer, **Demo window** double-tap the **Ctl Panel** icon and double-tap on **Touch Calibrate**. Follow the screen prompts.
	The system crashed.	Warm boot the system. To perform a warm boot, see *Resetting the Mobile Computer on page 1-11*.
A message appears stating that the mobile computer memory is full.	Too many files stored on the mobile computer.	Delete unused memos and records. If necessary, save these records on the host computer.
	Too many applications installed on the mobile computer.	Remove unused installed applications from the mobile computer to recover memory.

Table 8-1 Troubleshooting the Mobile Computer (Continued)

Problem	Cause	Solution
The mobile computer does not accept scan input.	Scanning application is not loaded.	Verify that the mobile computer is loaded with a scanning application.
	Unreadable bar code.	Ensure the symbol is not defaced.
	Distance between scan window and bar code is incorrect.	Ensure the mobile computer is within proper scanning range.
	Mobile computer is not programmed for the bar code type.	Ensure the mobile computer is programmed to accept the type of bar code scanned.
	Mobile computer 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.	Check the battery level. When the battery is low, the mobile computer automatically goes into suspend mode.

Single Slot Serial/USB Cradle

Table 8-2 Troubleshooting the Single Slot Serial/USB Cradle

Problem	Cause	Solution
Mobile computer amber Charge LED Indicator does not light when mobile computer inserted.	Cradle is not receiving power.	Ensure the power cable is connected securely to both the cradle and to AC power.
	Mobile computer is not correctly seated.	Remove and re-insert the mobile computer into the cradle, ensuring it is correctly seated.
Spare Battery Charging LED does not light when spare battery is inserted.	Spare battery is not correctly seated.	Remove and re-insert the spare battery into the charging slot, ensuring it is correctly seated.
Mobile computer battery is not charging.	Mobile computer was removed from cradle or cradle was unplugged from AC power too soon.	Ensure cradle is receiving power. Ensure the mobile computer is seated correctly. If the mobile computer battery is fully depleted, it can take up to four hours to fully recharge a Standard Battery and it can take up to six hours to fully recharge an Extended Life Battery.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	The mobile computer is not fully seated in the cradle.	Remove and re-insert the mobile computer into the cradle, ensuring it is correctly seated.

Table 8-2 Troubleshooting the Single Slot Serial/USB Cradle (Continued)

Problem	Cause	Solution
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 correctly 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.
During data communication, no data was transmitted, or transmitted data was incomplete.	Mobile computer removed from cradle during communication.	Replace mobile computer in cradle and retransmit.
	Incorrect cable configuration.	See *Chapter 2, Accessories* for cable configurations.
	Communication software is not installed or configured properly.	Perform communication setup as described in *Communication Setup on page 2-30.*

Four Slot Charge Only Cradle

Table 8-3 Troubleshooting the Four Slot Charge Only Cradle

Problem	Cause	Solution
Mobile computer amber Charge LED Indicator does not light when mobile computer inserted.	Cradle is not receiving power.	Ensure the power cable is connected securely to both the cradle and to AC power.
	Mobile computer is not correctly seated.	Remove and re-insert the mobile computer into the cradle, ensuring it is correctly seated.
Mobile computer battery is not charging.	Mobile computer was removed from cradle or cradle was unplugged from AC power too soon.	Ensure cradle is receiving power. Ensure mobile computer is seated correctly. If the mobile computer battery is fully depleted, it can take up to four hours to fully recharge a Standard Battery and it can take up to six hours to fully recharge an Extended Life Battery.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	The mobile computer is not fully seated in the cradle.	Remove and re-insert the mobile computer into the cradle, ensuring it is correctly seated.

Four Slot Ethernet Cradle

Table 8-4 Troubleshooting the Four Slot Ethernet Cradle

Problem	Cause	Solution
Mobile computer amber Charge LED Indicator does not light when mobile computer inserted.	Cradle is not receiving power.	Ensure the power cable is connected securely to both the cradle and to AC power.
	Mobile computer is not correctly seated.	Remove and re-insert the mobile computer into the cradle, ensuring it is correctly seated.
Mobile computer battery is not charging.	Mobile computer was removed from cradle or cradle was unplugged from AC power too soon.	Ensure cradle is receiving power. Ensure mobile computer is seated correctly. If the mobile computer battery is fully depleted, it can take up to four hours to fully recharge a Standard Battery and it can take up to six hours to fully recharge an Extended Life Battery.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	The mobile computer is not fully seated in the cradle.	Remove and re-insert the mobile computer into the cradle, ensuring it is correctly seated.
During data communication, no data was transmitted, or transmitted data was incomplete.	Mobile computer removed from cradle during communication.	Replace mobile computer in cradle and retransmit.
	Incorrect cradle setup.	See *Chapter 2, Accessories* for cradle setup.
	Ethernet connection error. Link LED is not lit (see *Link LED on page 2-11*).	Troubleshoot the Ethernet connection.

Four Slot Spare Battery Charger

Table 8-5 Troubleshooting the Four Slot Spare Battery Charger

Problem	Cause	Solution
Spare Battery Charging LED does not light when spare battery is inserted.	Spare battery is not correctly seated.	Remove and re-insert the spare battery into the charging slot, ensuring it is correctly seated.

Table 8-5 Troubleshooting the Four Slot Spare Battery Charger (Continued)

Problem	Cause	Solution
Battery not charging.	Charger is not receiving power.	Ensure the power cable is connected securely to both the charger and to AC power.
	Battery is not correctly seated.	Remove and re-insert the battery into the charger, ensuring it is correctly seated.
	Battery was removed from charger or charger was unplugged from AC power too soon.	Ensure charger is receiving power. Ensure the battery is seated correctly. If a battery is fully depleted, it can take up to four hours to fully recharge a Standard Battery and it can take up to six hours to fully recharge an Extended Life Battery.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.

UBC Adapter

Table 8-6 Troubleshooting the UBC Adapter

Problem	Cause	Solution
Spare battery Charging LED does not light when spare battery is inserted.	Spare battery is not correctly seated.	Remove and re-insert the spare battery into the charging slot, ensuring it is correctly seated.
Battery not charging.	Charger is not receiving power.	Ensure the power cable is connected securely to both the charger and to AC power.
	Spare battery is not correctly seated.	Remove and re-insert the spare battery into the charger, ensuring it is correctly seated.
	Battery was removed from charger or charger was unplugged from AC power too soon.	Ensure charger is receiving power. Ensure the battery is seated correctly. If a battery is fully depleted, it can take up to four hours to fully recharge a Standard Battery and it can take up to six hours to fully recharge an Extended Life Battery.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.

Cables

Table 8-7 Troubleshooting the Cables

Problem	Cause	Solution
Mobile computer amber Charge LED Indicator does not light when mobile computer attached.	Cable is not receiving power.	Ensure the power cable is connected securely to both the cable and to AC power.
	Mobile computer is not seated correctly in the cable.	Remove and re-insert the mobile computer into the MC3000 connector, ensuring it is correctly seated.
Mobile computer battery is not charging.	Mobile computer was detached from cable or cable was unplugged from AC power too soon.	Ensure the cable is receiving power. Ensure mobile computer is seated correctly. If the mobile computer battery is fully depleted, it can take up to four hours to fully recharge a Standard Battery and it can take up to six hours to fully recharge an Extended Life Battery.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	The mobile computer is not fully seated in the cable.	Remove and re-insert the mobile computer into the cable, ensuring it is correctly seated.
During data communication, no data was transmitted, or transmitted data was incomplete.	Cable removed from mobile computer during communication.	Reattach cable to mobile computer and retransmit.
	Incorrect cable configuration.	See *Chapter 2, Accessories* for cable configurations.
	Communication software is not installed or configured properly.	Perform communication setup as described in *Communication Setup on page 2-30*.

Appendix B Internet Explorer Kiosk Mode

Introduction

NOTE Kiosk Mode is available with OEM versions 05.26.000 and higher only.

The Kiosk Mode feature of Internet Explorer provides for configuration of the **Internet Explorer** window to display various menu and status bars.

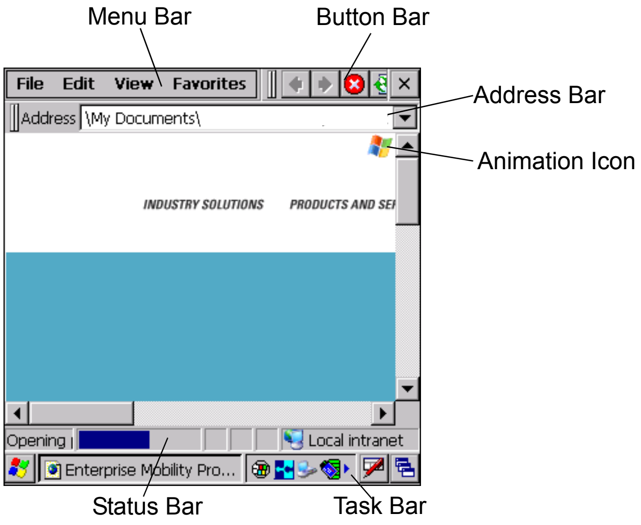


Figure B-1 *Internet Explorer Window*

Configuration is done through the registry settings: HKEY_CURRENT_USER > Software > Microsoft > Internet Explorer > Main.

The following registry keys are used to configure Kiosk mode:

- *URL* - hides/displays the Address bar.
- *Menu Bar* - hides/displays the Menu bar.
- *Button Bar* - hides/displays the Button bar.

- *Command Bar* - hides/displays the Address, Menu and Button bars.
- *Status Bar* - hides/displays the Status bar.
- *Task Bar* - hides/displays the Task bar.
- *Animation* - hides/displays the Animation icon.

Default value for each of the registry keys is: dword: 1.

NOTE After changing the registry entries close Internet Explorer and reopen it again for the application to take the modified registry values.

By default, all items listed above are visible. Setting the appropriate registry keys (dword: 1) disable the appropriate feature.

The Command bar contains the Menu bar, Button bar and Address bar. The *Command Bar* registry option overrides the *Menu Bar*, *Button Bar*, and *Address Bar* registry options. When the *Command Bar* registry value is 0 and if M*enu Bar*, *Button Bar* or *Address Bar* option is set to 1 then the whole *Command Bar* is hidden.

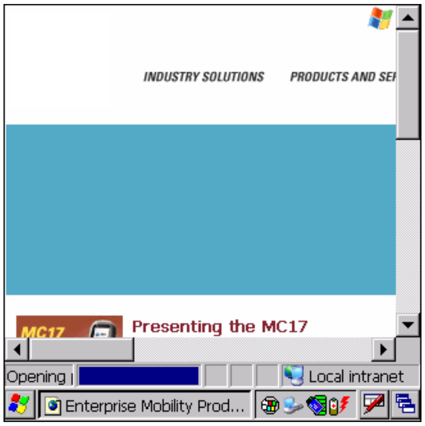


Figure B-2 *Internet Explorer with Command Bar Hidden*

NOTE When the Command bar is hidden, the only way to exit **Internet Explorer** is to end the task.

To make only the Menu bar visible, set the following:

- *Command Bar* = 1
- *Button Bar* = 0
- *URL* =0
- *Menu Bar* =1.

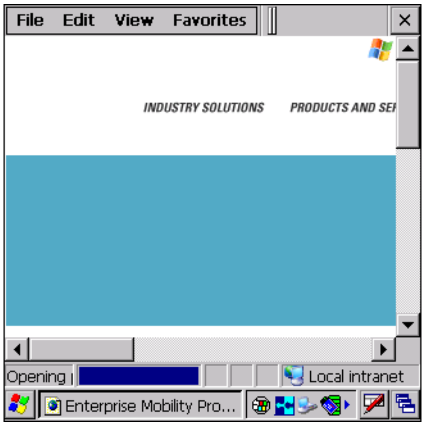

File Edit View Favorites
INDUSTRY SOLUTIONS PRODUCTS AND SEI
Opening
Local intranet
Enterprise Mobility Pro...

Figure B-3 *Internet Explorer with Menu Bar Visible*

To make only the Address bar visible, set the following:

- *Command Bar* = 1
- *Button Bar* = 0
- *URL* = 1
- *Menu Bar* = 0.

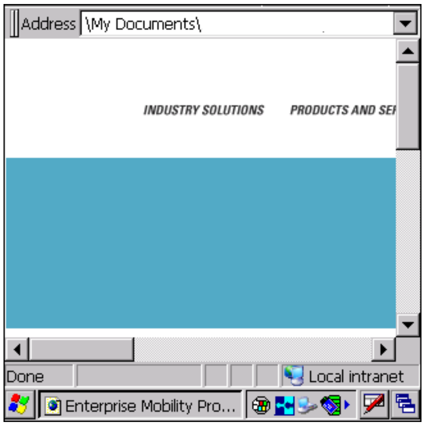

Address \My Documents\
INDUSTRY SOLUTIONS PRODUCTS AND SEI
Done
Local intranet
Enterprise Mobility Pro...

Figure B-4 *Internet Explorer with Address Bar Visible*

To make only the Button bar visible, set the following:

- *Command Bar* = 1
- *Button Bar* = 1
- *URL* = 0
- *Menu Bar* = 0.

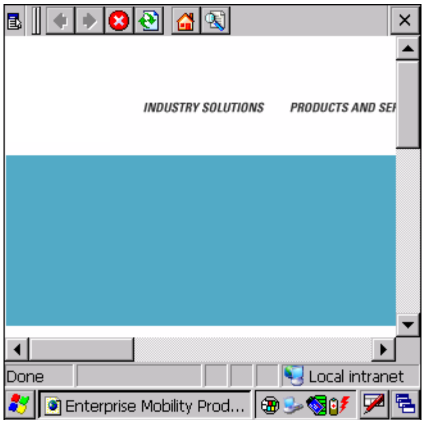


Figure B-5 *Internet Explorer with Button Bar Visible*

The bottom part of the **Internet Explorer** window contains the Status bar.

To hide the Status bar, set the following:

- *Status* = 0.

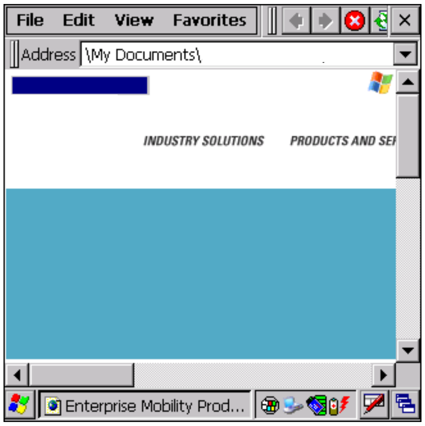


Figure B-6 *Internet Explorer with Status Bar Hidden*

The Taskbar at the bottom of the display can be hidden so that the **Internet Explorer** window fulls the entire display. To hide the Taskbar, set the following:

- *Task Bar* = 0.

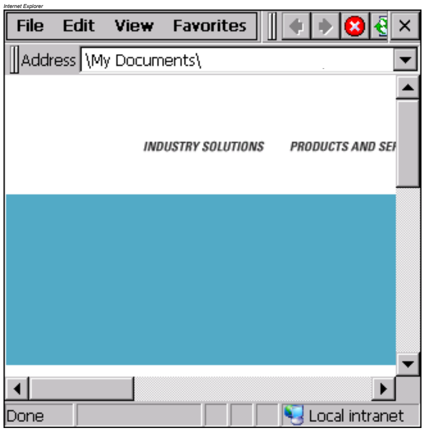


Figure B-7 *Internet Explorer with Task Bar Hidden*

To hide both the Status bar and the Taskbar, set the following:

- *Status Bar* = 0.
- *Task Bar* = 0.

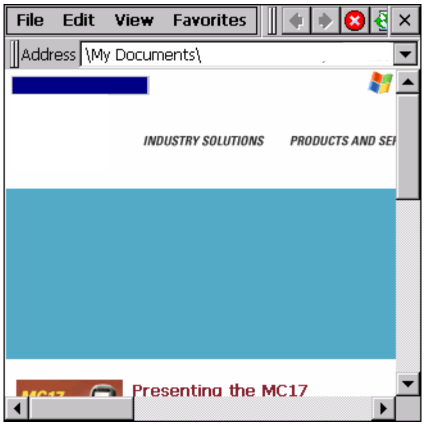
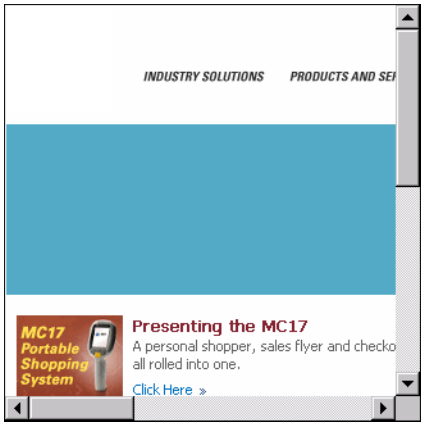


Figure B-8 *Internet Explorer with Status and Task Bar Hidden*

To hide all, set the following:

- *Command Bar* = 0
- *Status Bar* = 0
- *Task Bar* = 0



Presenting the MC17

A personal shopper, sales flyer and checko all rolled into one.

Click Here »

Figure B-9 *Internet Explorer with All Hidden*

The Animation icon display in the upper right corner of the window to indicate that **Internet Explorer** is accessing a web page. To hide the icon, set the following:

- *Animation* = 1

Glossary

Numeric

802.11/802.11abg. A radio protocol that may be used by the Zebra radio card.

A

Access Point. Access Point (AP) refers to Zebra's Ethernet Access Point. It is a piece of communications equipment that manages communications between the host computer system and one or more wireless terminals. An AP connects to a wired Ethernet LAN and acts as a bridge between the Ethernet wired network and IEEE 802.11 interoperable radio-equipped mobile units, such as a mobile computer. The AP allows a mobile user to roam freely through a facility while maintaining a seamless connection to the wired network.

AirBEAM® Manager. AirBEAM® Manager is a comprehensive wireless network management system that provides essential functions that are required to configure, monitor, upgrade and troubleshoot the wireless network and its components (including networked mobile computers). Some features include event notification, access point configuration, diagnostics, statistical reports, auto-discovery, wireless proxy agents and monitoring of access points and mobile units.

AirBEAM® Smart Client. AirBEAM® Smart Client is part of Zebra's AirBEAM® suite, which also includes AirBEAM® Safe and AirBEAM® Manager. The AirBEAM® Smart Client system uses the network accessible host server to store software files that are to be downloaded to the mobile computers. The AirBEAM® Smart Client provides the mobile computers with the "smarts" to request software from the host. It allows them to request, download and install software, as well as to upload files and status data. The AirBEAM® Smart Client uses the industry standard FTP or TFTP file transfer protocols to check the host system for updates, and if necessary, to transfer updated software. Most often, AirBEAM® Smart Client is used with wireless networks, but any TCP/IP connection can be used. For more information, refer to the AirBEAM® Smart Windows® CE Client Product Reference Guide (p/n 72-63060-xx).

AP. See **Access Point**.

Aperture. The opening in an optical system defined by a lens or baffle that establishes the field of view.

ASCII. American Standard Code for Information Interchange. A 7 bit-plus-parity code representing 128 letters, numerals, punctuation marks and control characters. It is a standard data transmission code in the U.S.

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. The dark element in a printed bar code symbol.

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**.

Bar Code Density. The number of characters represented per unit of measurement (e.g., characters per inch).

Bar Height. The dimension of a bar measured perpendicular to the bar width.

Bar Width. Thickness of a bar measured from the edge closest to the symbol start character to the trailing edge of the same bar.

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.

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

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.

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.

Codabar. A discrete self-checking code with a character set consisting of digits 0 to 9 and six additional characters: (“-”, “$”, “:”, “/”, “,” and “+”).

Code 128. A high density symbology which allows the controller to encode all 128 ASCII characters without adding extra symbol elements.

Code 3 of 9 (Code 39). A versatile and widely used alphanumeric bar code symbology with a set of 43 character types, including all uppercase letters, numerals from 0 to 9 and 7 special characters (“-”, “.”, “/”, “+”, “%”, “$” and space). The code name is derived from the fact that 3 of 9 elements representing a character are wide, while the remaining 6 are narrow.

Code 93. An industrial symbology compatible with Code 39 but offering a full character ASCII set and a higher coding density than Code 39.

Code Length. Number of data characters in a bar code between the start and stop characters, not including those characters.

Cold Boot. A cold boot restarts the mobile computer 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

Dead Zone. An area within a scanner's field of view, in which specular reflection may prevent a successful decode.

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.

Discrete Code. A bar code or symbol in which the spaces between characters (intercharacter gaps) are not part of the code.

Discrete 2 of 5. A binary bar code symbology representing each character by a group of five bars, two of which are wide. The location of wide bars in the group determines which character is encoded; spaces are insignificant. Only numeric characters (0 to 9) and START/STOP characters may be encoded.

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.

Element. Generic term for a bar or space.

EMDK. Enterprise Mobility Developer’s Kit.

Encoded Area. Total linear dimension occupied by all characters of a code pattern, including start/stop characters and data.

ESD. Electro-Static Discharge

ESN. Electronic Serial Number. The unique hardware number associated with a cellular device, which is transmitted to the system when the device communicates with the cellular system.

Ethernet. Ethernet communication port. Allows a wired interface to a radio network.

F

Flash Memory. Flash memory is nonvolatile, semi-permanent storage that can be electronically erased in the circuit and reprogrammed. Some mobile computers use Flash memory to store the operating system (ROM-DOS), the terminal emulators, and the Citrix ICA Client for DOS.

FTP. See **File Transfer Protocol**.

Flash Memory. Flash memory is responsible for storing the system firmware and is non-volatile. If the system power is interrupted the data is not be lost.

G

Gateway Address. An IP address for a network gateway or router. A mobile computer may be part of a subnet as specified by its IP address and Netmask. It can send packets directly to any node on the same subnet. If the destination node is on a different subnet, then the terminal sends the packet to the gateway first. The gateway determines how to route the packet to the destination subnet. This field is an option used by networks that require gateways.

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

IDE. Intelligent drive electronics. Refers to the solid-state hard drive type.

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.

Interleaved 2 of 5. A binary bar code symbology representing character pairs in groups of five bars and five interleaved spaces. Interleaving provides for greater information density. The location of wide elements (bar/spaces) within each group determines which characters are encoded. This continuous code type uses no intercharacter spaces. Only numeric (0 to 9) and START/STOP characters may be encoded.

imaging scanning . Mobile computers with an integrated imager use digital camera technology to take a digital picture of a bar code, store the resulting image in memory and execute state-of-the-art software decoding algorithms to extract the data from the image.

Intercharacter Gap. The space between two adjacent bar code characters in a discrete code.

Interleaved Bar Code. A bar code in which characters are paired together, using bars to represent the first character and the intervening spaces to represent the second.

Interleaved 2 of 5. A binary bar code symbology representing character pairs in groups of five bars and five interleaved spaces. Interleaving provides for greater information density. The location of wide elements (bar/spaces) within each group determines which characters are encoded. This continuous code type uses no intercharacter spaces. Only numeric (0 to 9) and START/STOP characters may be encoded.

Internet Protocol Address. See **IP**.

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.

L

LAN. Local area network. A radio network that supports data communication within a local area, such as within a warehouse of building.

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.

Laser Diode. A gallium-arsenide semiconductor type of laser connected to a power source to generate a laser beam. This laser type is a compact source of coherent light.

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.

Light Emitting Diode. See **LED**.

M

MC. Mobile Computer.

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.

Misread (Misdecode). A condition which occurs when the data output of a reader or interface controller does not agree with the data encoded within a bar code symbol.

Mobile Computer. In this text, *mobile computer* refers to the Zebra wireless handheld 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.

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.

P

Parameter. A variable that can have different values assigned to it.

PDT. Portable Data Terminal.

Percent Decode. The average probability that a single scan of a bar code would result in a successful decode. In a well-designed bar code scanning system, that probability should approach near 100%.

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.

Reflectance. Amount of light returned from an illuminated surface.

Resolution. The narrowest element dimension which is distinguished by a particular reading device or printed with a particular device or method.

RF. Radio Frequency.

ROM. Read-Only Memory. Data stored in ROM cannot be changed or removed.

ROM-DOS. The name of the licensed Disk Operating System loaded into the terminal's flash file system.

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**.

RS232. 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

Scan Area. Area intended to contain a symbol.

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

Self-Checking Code. A symbology that uses a checking algorithm to detect encoding errors within the characters of a bar code symbol.

Shared Key. Shared Key authentication is an algorithm where both the AP and the MU share an authentication key.

SID. System Identification code. An identifier issued by the FCC for each market. It is also broadcast by the cellular carriers to allow cellular devices to distinguish between the home and roaming service.

Soft Reset. See **Warm Boot**.

Space. The lighter element of a bar code formed by the background between bars.

Specular Reflection. The mirror-like direct reflection of light from a surface, which can cause difficulty decoding a bar code.

Start/Stop Character. A pattern of bars and spaces that provides the scanner with start and stop reading instructions and scanning direction. The start and stop characters are normally to the left and right margins of a horizontal code.

STEP. Symbol Terminal Enabler Program.

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.

SVTP. Symbol Virtual Terminal Program.

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.

Symbol Aspect Ratio. The ratio of symbol height to symbol width.

Symbol Height. The distance between the outside edges of the quiet zones of the first row and the last row.

Symbol Length. Length of symbol measured from the beginning of the quiet zone (margin) adjacent to the start character to the end of the quiet zone (margin) adjacent to a stop character.

Symbology. The structural rules and conventions for representing data within a particular bar code type (e.g. UPC/EAN, Code 39, PDF417, etc.).

T

Tolerance. Allowable deviation from the nominal bar or space width.

U

UPC. Universal Product Code. A relatively complex numeric symbology. Each character consists of two bars and two spaces, each of which is any of four widths. The standard symbology for retail food packages in the United States.

V

Visible Laser Diode (VLD). A solid state device which produces visible laser light.

W

WAN. Wide-Area Network. A radio network that supports data communication beyond a local area. That is, information can be sent across a city, state, or even nationwide.

Warm Boot. A warm boot restarts the mobile computer by closing all running programs. All data that is not saved to flash memory is lost.

Wireless Local Area Network (WLAN). See **LAN**.

Wireless Wide Area Network (WWAN). See **WAN**.

WNMP. (Wireless Network Management Protocol) This is a proprietary MAC layer protocol used for inter access point communication and other MAC layer communication.

Index

ZEBRA

Zebra Technologies Corporation
Lincolnshire, IL U.S.A
http://www.zebra.com

72E-68900-06 Revision A - April, 2015