MC909X Mobile Computer

Integrator Guide

MC909X Integrator Guide

Patents

This product is covered by one or more of the patents listed on the website: www.symbol.com/patents

Revision History

Changes to the original manual are listed below:

Change	Date	Description
Rev A	11/1/05	Initial release.
-02 Rev A	1/19/06	Add MC9090-K/S, MC9090-G and MC9094-K/S with Windows Mobile 5.0.
-03 Rev A	3/21/06	Add MC9097 support.
-04 Rev A	3/6/07	Add generic MC9097 information, 33-key keypad, Fusion 2.5 and AKU 3.2 update information.
-05 Rev A	9/15/07	Guide re-branding, incorporate Mobile OEM version 01.39.0001 and CE OEM version 01.26.0001 and add support for Haz Loc configurations.

Table of Contents

Chapter 4: Wireless Applications

Chapter 5: MC9094 Configuration

Chapter 6: MC9097 Configuration

Chapter 10: Maintenance & Troubleshooting

Appendix A: Technical Specifications

Appendix B: Using iDockIt

Glossary

Index

About This Guide

Introduction

This guide provides information about setting up and configuring MC909X mobile computers and accessories.

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

Documentation Set

The documentation set for the MC909X is divided into guides that provide information for specific user needs.

- **Microsoft Application Guide** - describes how to use Microsoft developed applications.
- **Symbol Application Guide** - describes how to use Symbol developed applications.
- **MC909X User Guide** - describes how to use the MC909X mobile computer.
- **MC909X Integrator Guide** - describes how to set up the MC909X mobile computer and the accessories.
- **SMDK Help File** - provides API information for writing applications.

User Types

End-User   Integrator   Application Developer

SMDK for C

SMDK Help File

Packaging, Symbol Web Site

Microsoft Application Guide

Symbol Application Guide

Integrator Guide

User Guide

Quick Start Guide
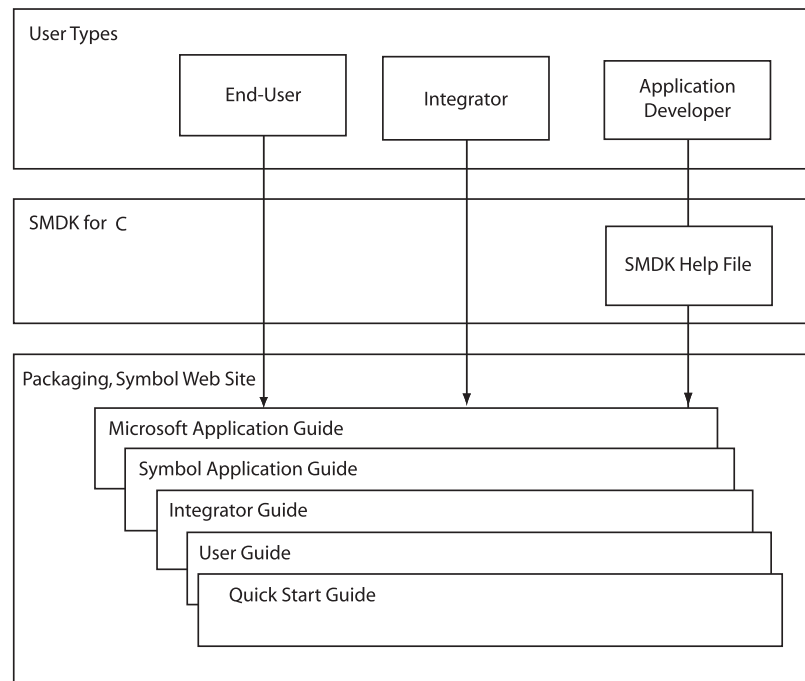
Configurations

This guide covers the following configurations:

Configuration	Radios	Display	Memory	Data Capture	Operating System	Keypads	Other
MC9090-G	WLAN: 802.11a/b/g WPAN: Bluetooth	Color or monochrome	64 MB RAM or 128 MB RAM/ 64 MB Flash	Laser, Long Range Laser, or Imager	Windows CE 5.0	28-key, 43-key, 53-key, VT, 3270, 5250 Emulators	Haz Loc Class 1 Div 2 Condensation Resistant[1]
MC9090-G	WLAN: 802.11a/b/g WPAN: Bluetooth	Color	64 MB RAM or 128 MB RAM/ 128 MB Flash	Laser, Long Range Laser, or Imager	Windows Mobile 5.0 Premium Edition	28-key, 43-key, 53-key, VT, 3270, 5250 Emulators	Haz Loc Class 1 Div 2 Condensation Resistant[1]
MC9090-K	WLAN: 802.11a/b/g WPAN: Bluetooth	Color	64 MB RAM or 128 MB RAM/ 128 MB Flash	Laser or Imager	Windows Mobile 5.0 Premium Edition	28-key, 33-key, 43-key, 53-key	Haz Loc Class 1 Div 2
MC9090-S	WLAN: 802.11a/b/g WPAN: Bluetooth	Color	64 MB RAM or 128 MB RAM/ 128 MB Flash	Laser or Imager	Windows Mobile 5.0 Premium Edition	28-key, 38-key alpha, 38-key numeric	
MC9094-K	WLAN 802.11a/b/g WPAN: Bluetooth WWAN:EDGE/ GPRS	Color	64 MB RAM or 128 MB RAM/ 128 MB Flash	Laser or Imager	Windows Mobile 5.0 Phone Edition	28-key, 33-key, 43-key, 53-key	

[1] Condensation Resistant configurations utilize desiccant located inside the mobile computer to capture internal moisture that forms when they are carried from a warm humid environment to a cold environment.

Configuration	Radios	Display	Memory	Data Capture	Operating System	Keypads	Other
MC9094-S	WLAN 802.11a/b/g WPAN: Bluetooth WWAN:EDGE/GPRS	Color	64 MB RAM or 128 MB RAM/ 128 MB Flash	Laser or Imager	Windows Mobile 5.0 Phone Edition	28-key, 38-key alpha, 38-key numeric	
MC9097-K	WLAN 802.11a/b/g WPAN: Bluetooth WWAN: iDEN	Color	64 MB RAM or 128 MB RAM/ 128 MB Flash	Laser or Imager	Windows Mobile 5.0 Phone Edition	28-key, 33-key, 43-key, 53-key	
MC9097-S	WLAN 802.11a/b/g WPAN: Bluetooth WWAN: iDEN	Color	64 MB RAM or 128 MB RAM/ 128 MB Flash	Laser or Imager	Windows Mobile 5.0 Phone Edition	28-key, 38-key alpha, 38-key numeric	

¹ Condensation Resistant configurations utilize desiccant located inside the mobile computer to capture internal moisture that forms when they are carried from a warm humid environment to a cold environment.

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
- Phone version
- Fusion version.

AKU Version for Mobile 5.0 Devices

To determine the Adaptation Kit Update (AKU) version on a Mobile 5.0 device:

Tap **Start** > **Settings** > **System** tab > **About** icon > **Version** tab.
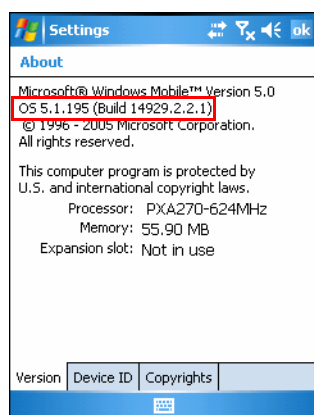
The second line lists the operating system version and the build number. The last part of the build number represents the AKU number. For example, *Build 14929.2.2.1* indicates that the device is running AKU version *2.2.1*.

OEM Version on Mobile 5.0 Devices

To determine the OEM software version on a Mobile 5.0 device:

Tap **Start** > **Settings** > **System** tab > **System Information** icon > **System** tab.
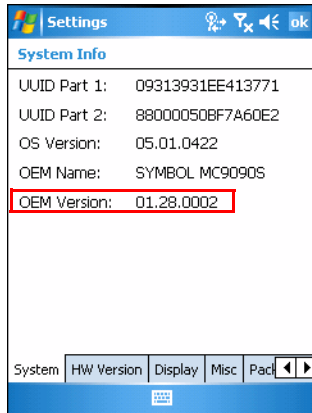
OEM Software on Windows CE 5.0 devices

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

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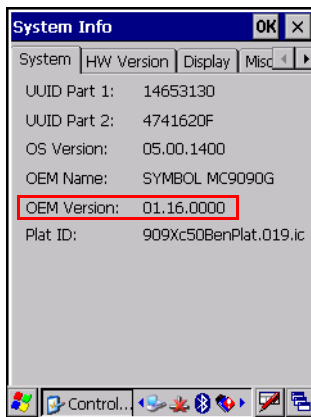
Fusion Software

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

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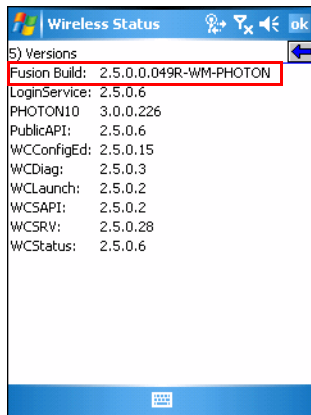
Phone Software

To determine the Phone software version on a Mobile 5.0 device:

Tap **Start** > **Phone** > **Menu** > **Options** > **Version Information** tab.

MC9094
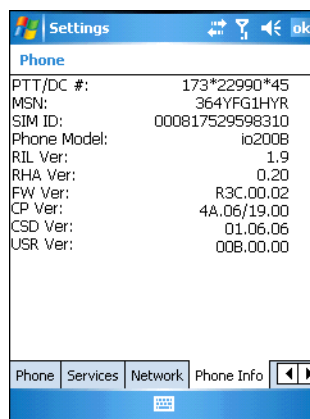
MC9097

Chapter Descriptions

Topics covered in this guide are as follows:

- *Chapter 1, Getting Started*, provides information on charging the mobile computer battery and resetting.

- *Chapter 2, Accessories*, describes the accessories available for the mobile computer and how to set up power connections and battery charging capabilities, where applicable.

- *Chapter 3, ActiveSync*, provides instructions on installing ActiveSync and setting up a partnership between the mobile computer and a host computer.

- *Chapter 4, Wireless Applications*, provides instructions using and configuring the mobile computer on a wireless network.

- *Chapter 5, MC9094 Configuration*, describes how to configure the WWAN MC9094 phone connection.

- *Chapter 6, MC9097 Configuration*, describes how to configure the WWAN MC9097 phone connection.

- *Chapter 7, Application Deployment for WinCE 5.0*, provides instructions for installing the Device Configuration Package (DCP) for MC909X and the SMDK for C on the host computer and downloading software and files to the mobile computer.

- *Chapter 8, Application Deployment for Mobile 5.0*, describes new features in Windows Mobile 5.0 including new security features, how to package applications, and procedures for deploying applications onto the mobile computer.

- *Chapter 9, Staging and Provisioning*, explains how to facilitate software downloads to the mobile computer.

- *Chapter 10, 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, Using iDockIt*, provides *iDockIT* software operating instructions.

Notational Conventions

The following conventions are used in this document:

- "Mobile computer" refers to the Symbol MC909X series of hand-held computers.

- *Italics* are used to highlight the following:
  - Chapters and sections in this guide
  - Related documents

- **Bold** text is used to highlight the following:
  - Dialog box, window and screen names
  - Drop-down list and list box names
  - Check box and radio button names
  - Icons on a screen
  - Key names on a keypad
  - Button names on a screen.

- Bullets (•) indicate:
  - Action items
  - Lists of alternatives
  - Lists of required steps that are not necessarily sequential.

- Sequential lists (e.g., those that describe step-by-step procedures) appear as numbered lists.

Related Documents and Software

The following documents provide more information about the MC909X mobile computers.

- *MC9090-G Quick Start Guide,* p/n 72-72217-xx

- *MC909X-K/S Quick Start Guide,* p/n 72-72220-xx

- *MC9097-K/S Quick Start Guide,* p/n 72-72221-xx

- *MC9090-G Windows® Mobile® 5.0 Regulatory Guide*, p/n 72-72219-xx

- *MC9090-G Windows® CE 5.0 Regulatory Guide*, p/n 72-72218-xx

- *MC909X-K/S Windows® Mobile® 5.0 Regulatory Guide*, p/n 72-73446-xx

- *MC909X User Guide*, p/n 72E-72215-xx

- *Symbol Application Guide for Symbol Devices*, p/n 72E-68901-xx

- *Microsoft Applications for Mobile and WinCE 5.0 User Guide*, p/n 72E-78456-xx

- *Symbol Mobility Developer Kit (SMDK) Help File*, p/n 72E-38880-03

- *Symbol Mobility Developer Kits,* available at: http://support.symbol.com

- Device Configuration Package (DCP for MC9090c50) and Platform SDK (PSDK9090c50) for MC9090-G with Windows CE 5.0, available at: http://support.symbol.com.

- ActiveSync software, available at: http://www.microsoft.com.

For the latest version of this guide and all guides, go to: http://support.symbol.com.

Service Information

If you have a problem with your equipment, contact the "Symbol Global Interactive Center," for your region. Go to http://www.symbol.com/contactsupport. If you purchased your Symbol product from a Symbol Business Partner, contact that Business Partner for service.

Before contacting, have the model number and serial number at hand. If your problem cannot be solved by the Symbol Global Interactive Center, you may need to return your equipment for servicing and you will be given specific directions.

Motorola 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.

Chapter 1 Getting Started

Introduction

This chapter lists the accessories for the mobile computer and explains how to install and charge the batteries, replace the strap and 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 you received all equipment listed below:

- mobile computer
- lithium-ion battery
- strap, attached to the mobile computer
- stylus, in the stylus silo
- Regulatory Guide
- Quick Start Guide (poster).

Inspect the equipment for damage. If you are missing any equipment or if you find any damaged equipment, contact the Symbol Technologies Support Center immediately. See *Service Information on page xxi* for contact information.
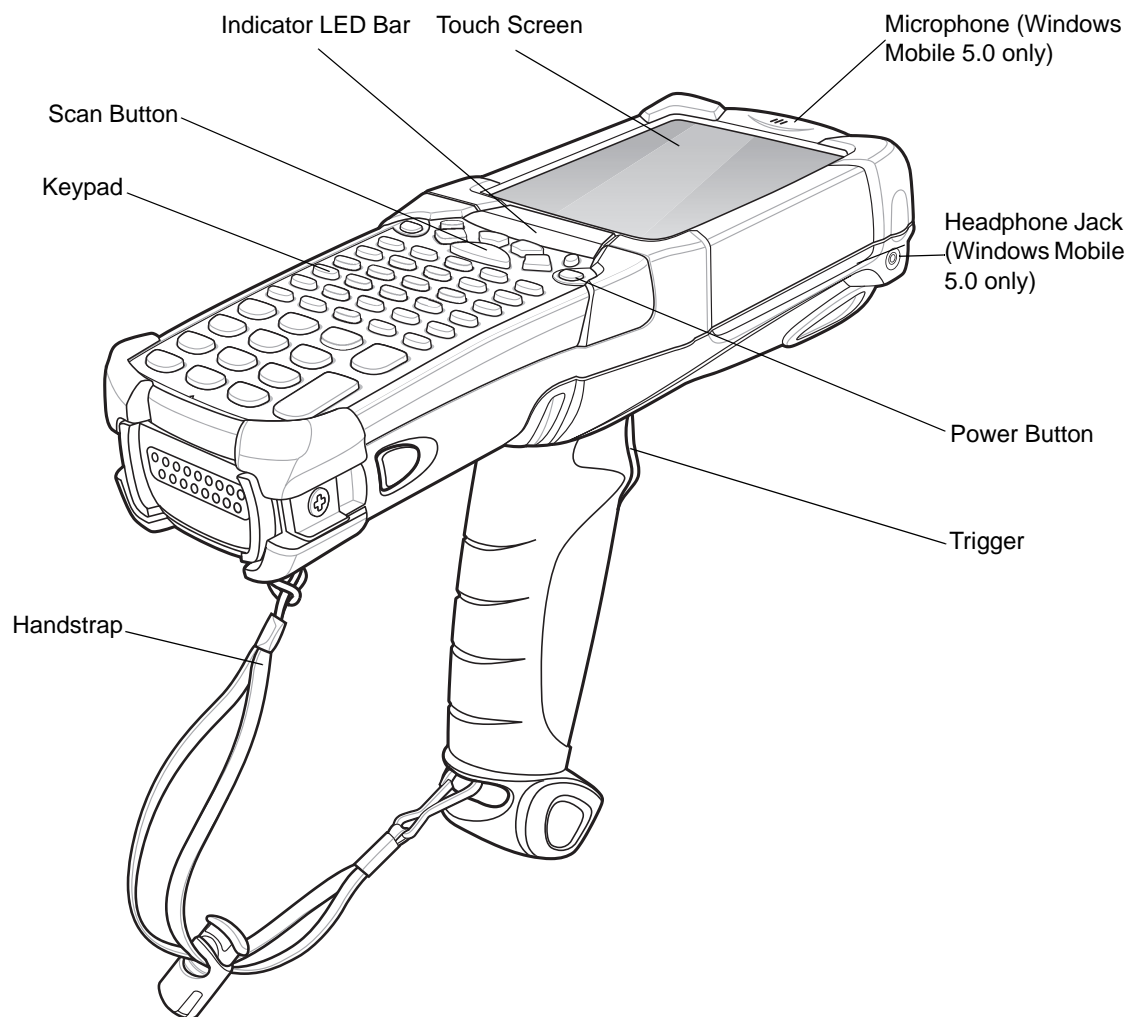
Figure 1-1   *MC9090-G*
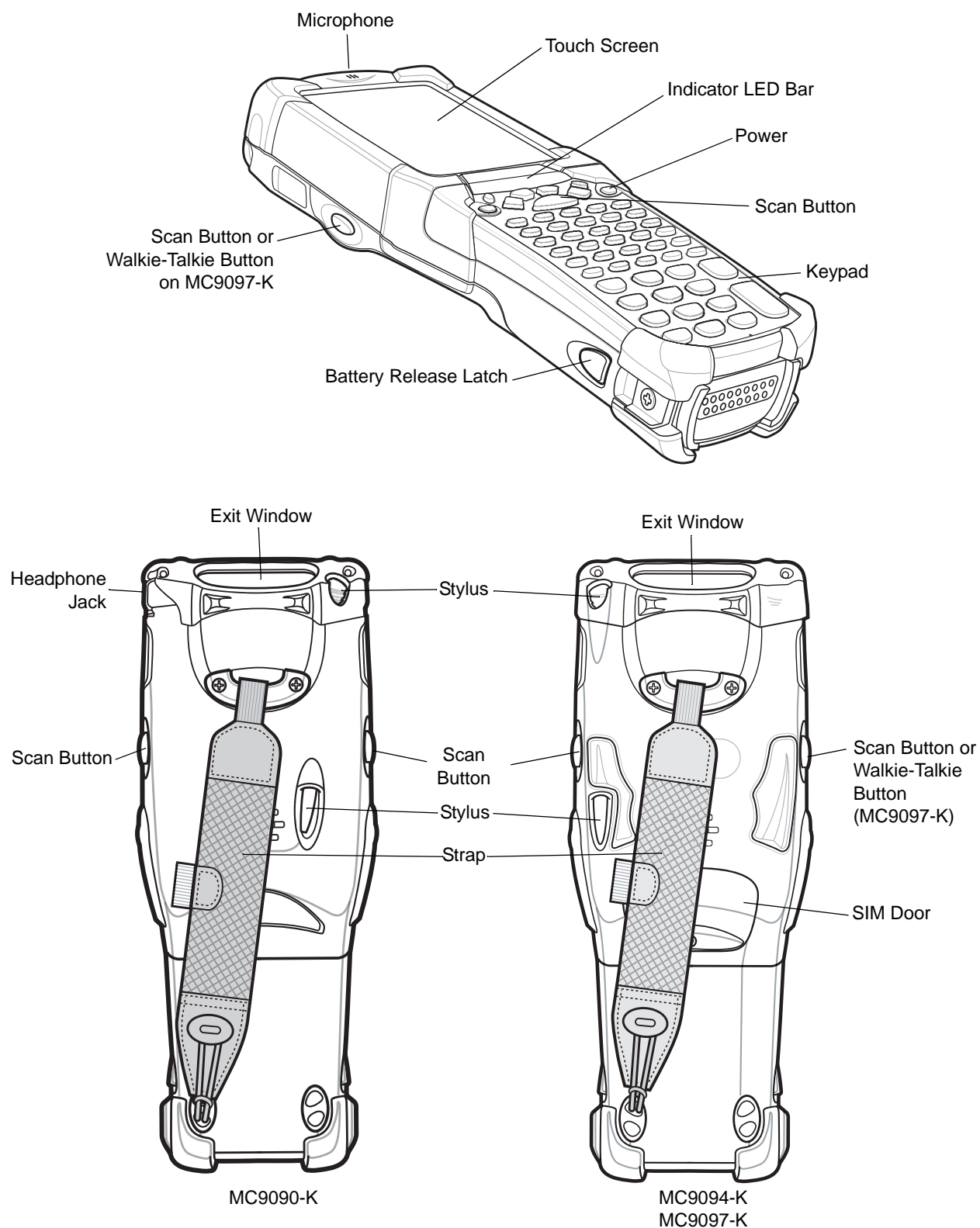
Figure 1-2   *MC909X-K*
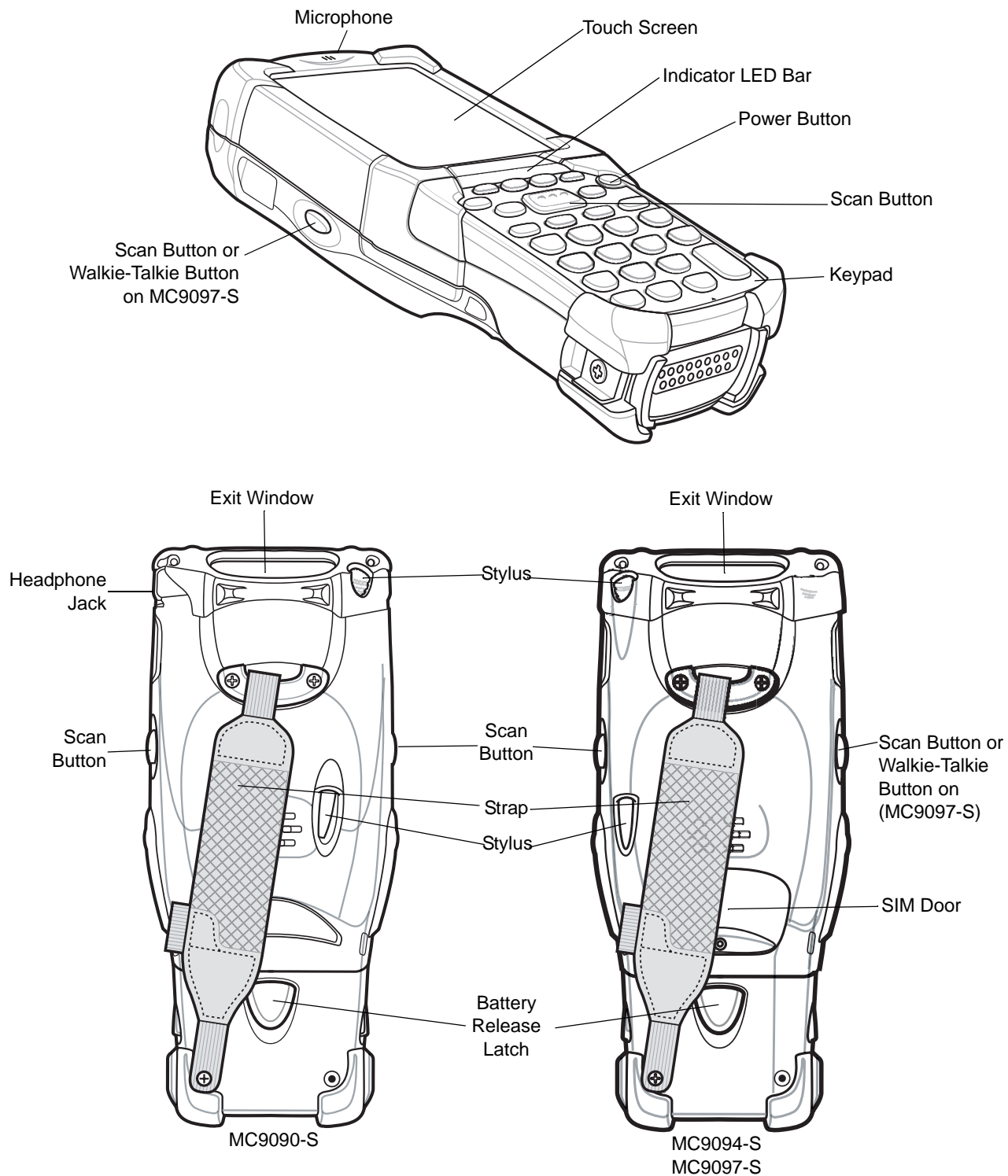
Figure 1-3 *MC909X-S*

Accessories

Table 1-1 lists the accessories available for the MC909X.

Table 1-1 *MC909X Accessories*

Accessory	Description
Cable Adapter Module (CAM)	Snap-on required to connect the following cables to the mobile computer. • AC line cord (country-specific) and power supply, charges the mobile computer. • Auto charge cable, charges the mobile computer using a vehicle's cigarette lighter. • DEX cable, connects the mobile computer to a vending machine. • Serial cable, adds serial communication capabilities. • USB cable, adds USB communication capabilities. • Printer cable, adds printer communication capabilities.
Four Slot Charge Only Cradle	Charges the mobile computer main battery.
Four Slot Ethernet Cradle	Charges the mobile computer main battery and synchronizes the mobile computer with a host computer through an Ethernet connection.
Vehicle Cradle	Installs in a vehicle and charges the mobile computer main battery and a spare battery. Provides serial data communication between the mobile computer and an external device.
Four Slot Spare Battery Charger	Charges up to four mobile computer spare batteries.
Headphones	Use in noisy environments.
Holster	Holds the mobile computer when not in use.
Keypads (Optional)	Application specific keypads.
Magnetic Stripe Reader (MSR)	Snaps on to the mobile computer and adds magstripe read capabilities.
Modem Module	Enables data communication between the mobile computer and a host computer, remotely through the phone lines, and synchronizes information between the mobile computer and a host computer.
Multimedia Card (MMC)	Provides secondary non-volatile storage.
Single Slot Serial/USB Cradle	Charges the mobile computer main battery and a spare battery. It also synchronizes the mobile computer with a host computer through either a serial or a USB connection.
Software	*Symbol Mobility Developer Kits* available at: http://support.symbol.com.
	Device Configuration Package (DCPforMC9090c50) and Platform SDK (PSDK9090c50) for MC9090-G with Windows CE 5.0 only, available at: http://support.symbol.com.
Spare lithium-ion battery	Replacement battery.

Table 1-1 *MC909X Accessories (Continued)*

Accessory	Description
Stylus	Performs pen functions.
Universal Battery Charger Adapter	Adapts the UBC for use with the Series 9000 batteries.
Wall Mounting Bracket and Shelf Slide	Use for wall mounting applications.

Getting Started

In order to start using the mobile computer for the first time:

- install the main battery
- charge the main battery and backup battery
- start the mobile computer
- configure the mobile computer.

The main battery can be charged before or after it is installed. 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 installed in the mobile computer.

Installing and Removing the Main Battery

Installing the Main Battery

Before using the mobile computer, install a lithium-ion battery by sliding the battery into the mobile computer as shown in *Figure 1-4*.

> *NOTE* Ensure the battery is fully inserted. Two audible clicks can be heard as the battery is fully inserted. A partially inserted battery may result in unintentional data loss.

When a battery is fully inserted in a mobile computer for the first time, upon the mobile computer's first power up, the device boots and powers on automatically.
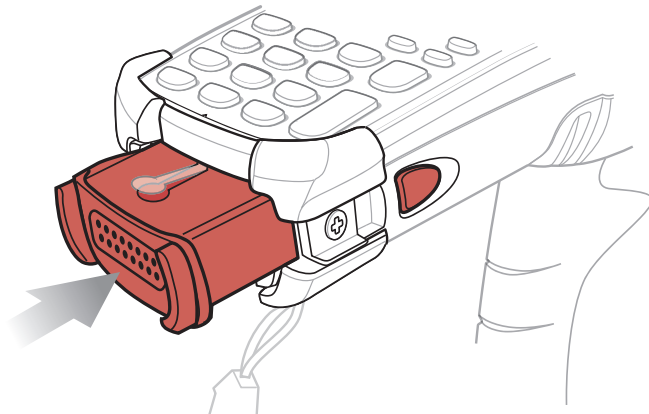
Figure 1-4   *Installing the Main Battery*

Charging the Battery

⚠️ **CAUTION**   Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 10-1*.

Charging the Main Battery and Memory Backup Battery

Before using the mobile computer for the first time, charge the main battery until the amber charge indicator light remains lit (see *Table 1-2 on page 1-8* for charge status indications). The main battery fully charges in less than four hours. The mobile computer can be charged using a cradle, the CAM, or the MSR with the appropriate power supply.

The mobile computer is also 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.

Use the following to charge batteries:

- Cradles: The mobile computer slips into the cradles for charging the battery in the mobile computer (and spare batteries, where applicable).
  - Single Slot Serial/USB Cradle.
  - Four Slot Ethernet Cradle and Four Slot Charge Only Cradles.

- Accessories: The mobile computer's snap-on accessories provide charging capability, when used with one of the accessory charging cables.
    - CAM
    - MSR.

- Chargers: The mobile computer's spare battery charging accessories are used to charge batteries that are removed from the mobile computer.
    - Single Slot Serial/USB Cradle
    - Four Slot Spare Battery Charger
    - Universal Battery Charger (UBC).

> **NOTE** To achieve the best battery life in mobile computers with multiple radios, turn off the radios that are not being used. See *Turning Off the Radios on page 1-21* for more inofrmation.

Charging the Main Battery

Charge the main battery in the mobile computer using a cradle, the CAM with a charging cable, or the MSR with the appropriate power supply.

1. Ensure the accessory used to charge the main battery is connected to the appropriate power source (see *Chapter 2, Accessories* for setup information).

2. Insert the mobile computer into a cradle or attach the appropriate snap-on module.

3. The mobile computer starts to charge automatically. The amber charge LED, in the Indicator LED Bar, lights to show the charge status. See *Table 1-2* for charging indications.

The main battery usually fully charges in less than four hours.

Table 1-2 *Mobile Computer LED Charge Indicators*

LED	Indication
Off	Mobile computer not in cradle or the mobile computer is not attached to the CAM or MSR. Mobile computer not placed 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.

Charging Spare Batteries

⚠️ **CAUTION**   Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 10-1*.

Use the following three accessories to charge spare batteries:

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

To charge a spare battery:

1. Ensure the accessory used to charge the spare battery is connected to the appropriate power source (see *Chapter 2, Accessories* for setup information).

2. Insert the spare battery into the accessory's spare battery charging slot with the charging contacts facing down (over the charging pins) and gently press down on the battery to ensure proper contact.

3. The battery starts to charge automatically. The amber charge LED on the accessory lights to show the charge status. See *Chapter 2, Accessories* for charging indications for the accessory.

The battery usually fully charges in less than four hours.

Removing the Main Battery

To remove the main battery:

1. Prior to removing the battery, press the red **Power** button to place the mobile computer in the suspend mode.

2. For the MC9097, wait 10 seconds before proceeding to the next step. If you do not, you may need to perform a warm boot after replacing the battery.

3. Press the primary battery release(s). The battery partially ejects from the mobile computer.

4. Pause three to four seconds while the mobile computer performs battery removal shutdown.

5. Press the secondary battery release, on top of the battery, and slide the battery out of the mobile computer.
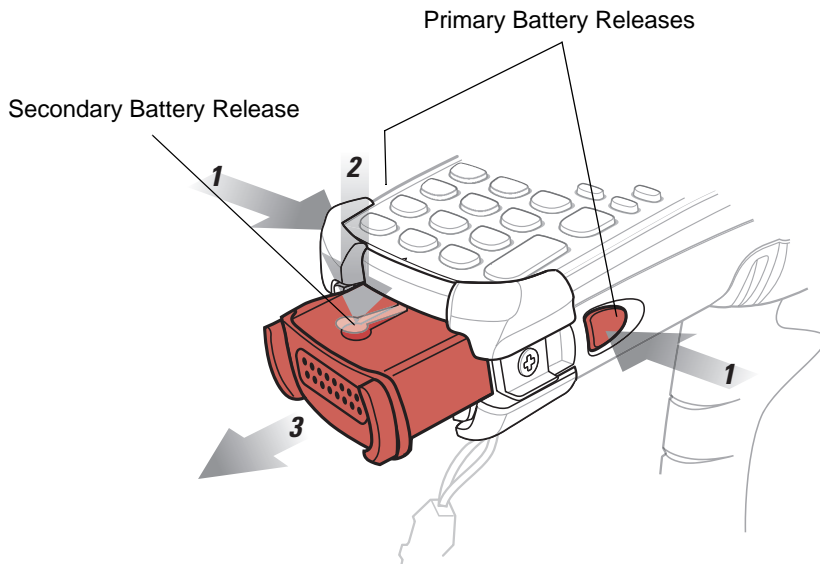
Figure 1-5   *Removing the Main Battery*
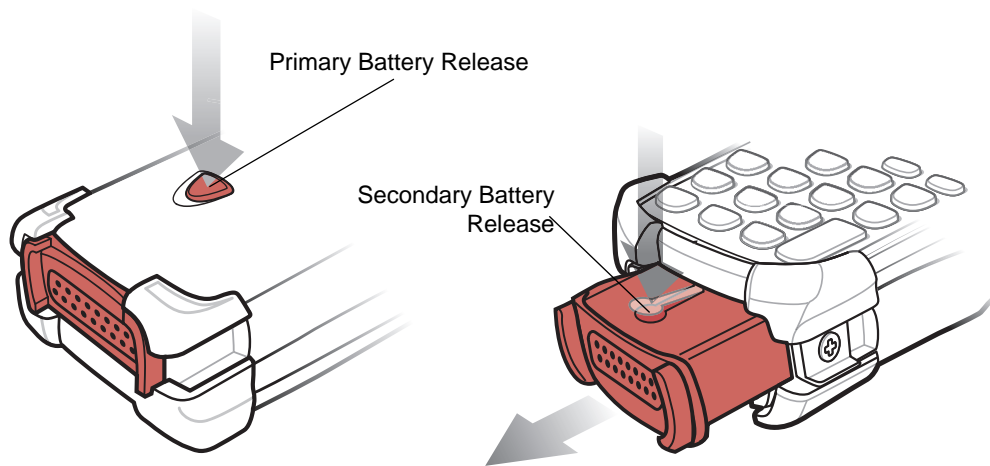
Figure 1-6   *Removing the Main Battery - MC909X-S*

Starting the Mobile Computer

Press the red **Power** button to turn on the mobile computer. If the mobile computer does not power on, perform a cold boot. See *Performing a Cold Boot on page 2-41*.

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

When the mobile computer is powered on for the first time, it initializes its system. The splash screen (*Figure 1-7*) appears for a short period of time.

MC9090/4   MC9097
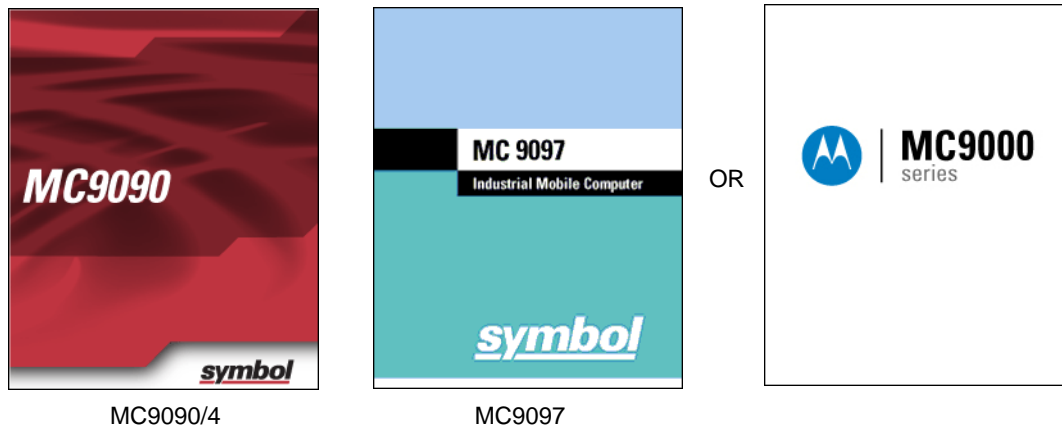
Figure 1-7   *Symbol Splash Window*

Calibrating the Screen

To calibrate the screen so that the cursor on the touch screen aligns with the tip of the stylus:

1.   Using the stylus carefully press and briefly hold the tip of stylus on the center of each target that appears on the screen.

    NOTE   To re-calibrate the screen at anytime, press Blue key + **ESC** on the mobile computer to launch the calibration screen application.

2.   Repeat as the target moves around the screen or press **ESC** to cancel.

Checking Battery Status

To check whether the main battery or backup battery in the mobile computer is charged, tap **Start** > **Settings** > **Control Panel** > **Power** icon to display the **Battery Status** window.

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

Configuring the Mobile Computer

- To customize the mobile computer settings, refer to the *Microsoft Applications for Mobile and CE 5.0 User Guide*.

- To set up ActiveSync to synchronize the mobile computer with the host computer, see *Chapter 3, ActiveSync*.

- To configure the mobile computer for wireless LAN network, see *Chapter 4, Wireless Applications*.

- To configure the mobile computer for WWAN network, see *Chapter 5, MC9094 Configuration*.

- To configure the mobile computer for iDEN network, see *Chapter 6, MC9097 Configuration*.

- To deploy software on the mobile computer, see *Chapter 7, Application Deployment for WinCE 5.0* or *Chapter 8, Application Deployment for Mobile 5.0*.

Resetting the Mobile Computer

Windows CE 5.0 Devices

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

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

Perform a warm boot first. This restarts the 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

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

Performing a Cold Boot

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

> **CAUTION**   Do not hold down any key, other than the **Power** button during a reset. Performing a cold boot restores formats, preferences and other settings to the default settings.

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

To perform a cold boot:

1. Press the primary battery release on the mobile computer to partially eject the battery from the mobile computer.

2. While the battery is partially released, simultaneously press and release the handle trigger and the **Power** button.

3. Push the battery to fully re-insert it in the mobile computer. One audible click can be heard as the battery is fully inserted.

4. The mobile computer initializes.

5. Calibrate the screen.

Windows Mobile 5.0 Devices

There are three reset functions, warm boot, cold boot and clean 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).

•   A clean boot resets the mobile computer to the factory default settings.

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

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

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.*

To perform a cold boot:

1.   Press the primary battery release on the mobile computer to partially eject the battery from the mobile computer.

2.   On an MC9090-G, while the battery is partially released, simultaneously press and release the trigger and the **Power** button.

     or

     On an MC-909X-K or MC909X-S, while the battery is partially released, simultaneously press and release the left scan button and the **Power** button.

3.   Push the battery to fully re-insert it in the mobile computer. One audible click can be heard as the battery is fully inserted.

4.   The mobile computer initializes.

Performing a Clean Boot

⚠	**CAUTION**	A clean boot should only be performed by an authorized system administrator. You must connect the mobile computer to AC power during a clean boot.
		Removing AC power from the mobile computer during a clean boot may render the mobile computer inoperable.

A clean boot resets the mobile computer to the factory default settings. All data is the **Application** folder is retained. You must download the Clean Boot Package file from the Symbol Support Central and install on the mobile computer.

To perform a clean boot:

1.   Download the Clean Boot Package from the Symbol Support Central. Follow the instructions included in the package for installing the package onto the mobile computer.

2.   Press the primary battery release on the mobile computer to partially eject the battery from the mobile computer.

3.   On an MC9090-G, while the battery is partially released, simultaneously press and release the trigger and the **Power** button.

     or

On an MC909X-K or MC909X-S, while the battery is partially released, simultaneously press and release the left scan button and the **Power** button.

NOTE   After you insert the battery you have two seconds to press the trigger or left scan button.

4. Push the battery to fully re-insert it in the mobile computer. One audible click can be heard as the battery is fully inserted.

5. On the MC9090-G, press and hold the trigger.

    or

    On the MC909X-K or MC909X-S, press and hold the left scan button.

6. Connect the mobile computer to AC power using the CAM or insert the mobile computer into a powered cradle.

7. The mobile computer updates and then re-boots.

8. The calibration screen appears.

SIM Card

NOTE   Subscriber Identification Module (SIM) card is only used in the MC9094 and MC9097 configurations.

The SIM card, or smart card, is required for MC9094 (GPRS) and MC9097 (iDEN) phone service. The SIM card for the MC9094 must be obtained from the phone service provider. The MC9097 comes from the factory with the inactive SIM card pre-installed. The card fits into the mobile computer and can contain the following information:

- Mobile phone service provider account details.
- Information regarding service access and preferences.
- Contact information, which can be moved to Contacts on the mobile computer.
- Any additional services to which the user may have subscribed.

NOTE   For more information about SIM cards, refer to the mobile phone service provider's documentation.

To install the SIM card:

1. Place the mobile computer into the suspend mode by pressing the red **Power** button.

2. Remove the SIM door on the back of the mobile computer.
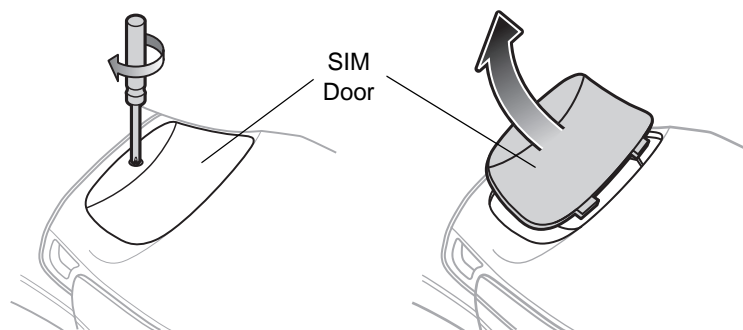
Figure 1-8   *Removing SIM Door*

3.   Unlock the SIM holder by sliding the metal clip to the open position.

4.   Lift the SIM holder.
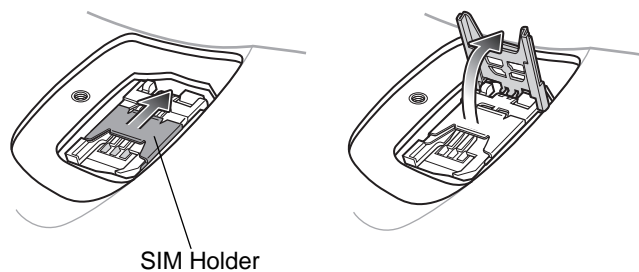
Figure 1-9   *Unlock SIM Case*

5.   Insert the SIM card, as shown in *Figure 1-10*, with the cut edge of the card facing the top of the mobile computer and the contacts facing down.

6.   Lower the SIM holder.
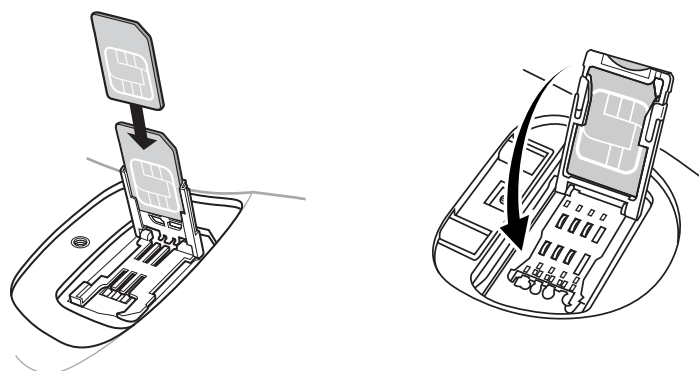
Figure 1-10   *Inserting the SIM Card*

7.   Lock the metal clip by sliding it to the closed position.
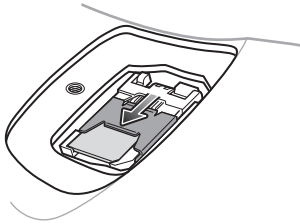
Figure 1-11   *Locking the SIM Card Housing*

8.   Replace the SIM door with one screw.
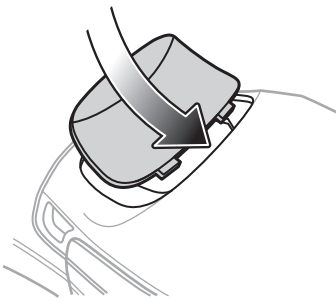
Figure 1-12   *Replacing the SIM Door*

9.   Press the red **Power** button.

> *NOTE*   On the MC9097, it is not recommended that you swap the SIM card with another SIM card. If you do swap SIM cards, perform step 10.

10.   On the MC9097, you must preform a master rest after installing a new SIM card.

    a.   Tap **Start** > **Phone** > **Menu** > **Options** > **Error Log** tab.

    b.   Tap the **Master Reset** button.

    c.   Tap **OK**.

    d.   Once an "X" appears in the Phone Antenna icon (wait a few seconds), perform a warm boot.

    e.   Wait for the mobile computer to reboot and then perform a second warm boot.

11.   Tap **Start** > **Phone** > **Menu** > **Options** > **Network** tab and verify that the service provider appears in the **Current network:** field.

12.   Make a call to verify connection.

> *NOTE*   For detailed information about WWAN activation and settings, refer to *Chapter 5, MC9094 Configuration* or *Chapter 6, MC9097 Configuration*.
>
> On the MC9097, if the SIM door is removed without removing the SIM card, you must warm boot the mobile computer.

Stylus

Use the mobile computer stylus for selecting items and entering information. The stylus functions as a mouse.

- Tap: Touch the screen once with the stylus to press option buttons and open menu items.

- Tap and Hold: Tap and hold the stylus on an item to see a list of actions available for that item. On the pop-up menu that appears, tap the action you want to perform.

- Drag: Hold the stylus on the screen and drag across the screen to select text and images. Drag in a list to select multiple items.

MC9090-G Strap

The strap may be moved to either the left or right side of the mobile computer to suit user preferences.

To reposition the strap:

1. Disconnect the metal clip at the handle.

2. Open strap loop and slide the handstrap through the loop.

3. Slide the loop out of the connector post.

4. Reverse the procedure to re-attach the strap. Two strap connectors are provided on the mobile computer's main body. The handstrap may be attached to either connector.

Strap Loop

Handstrap

Metal Clip
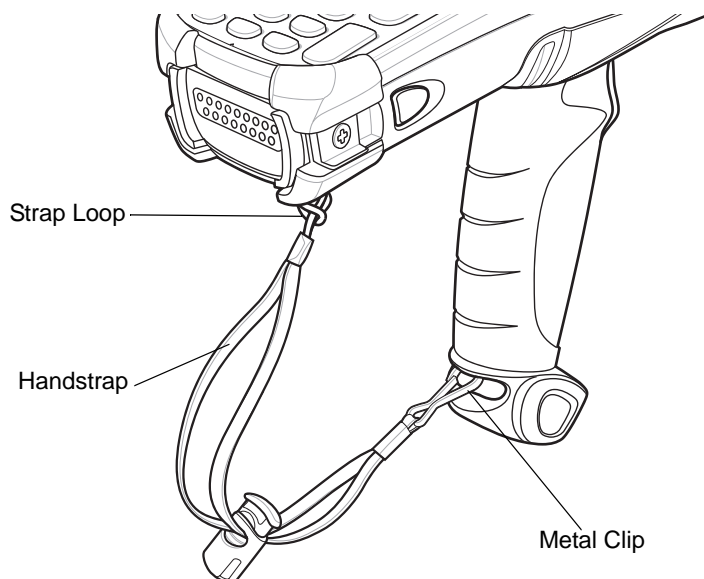
Figure 1-13   *Reposition the Strap*

MC909X-K Strap

The strap may be moved to either the left or right side of the mobile computer to suit user preferences. To reposition the MC909X-K strap:

1. Lift the loop end of the strap over the button.
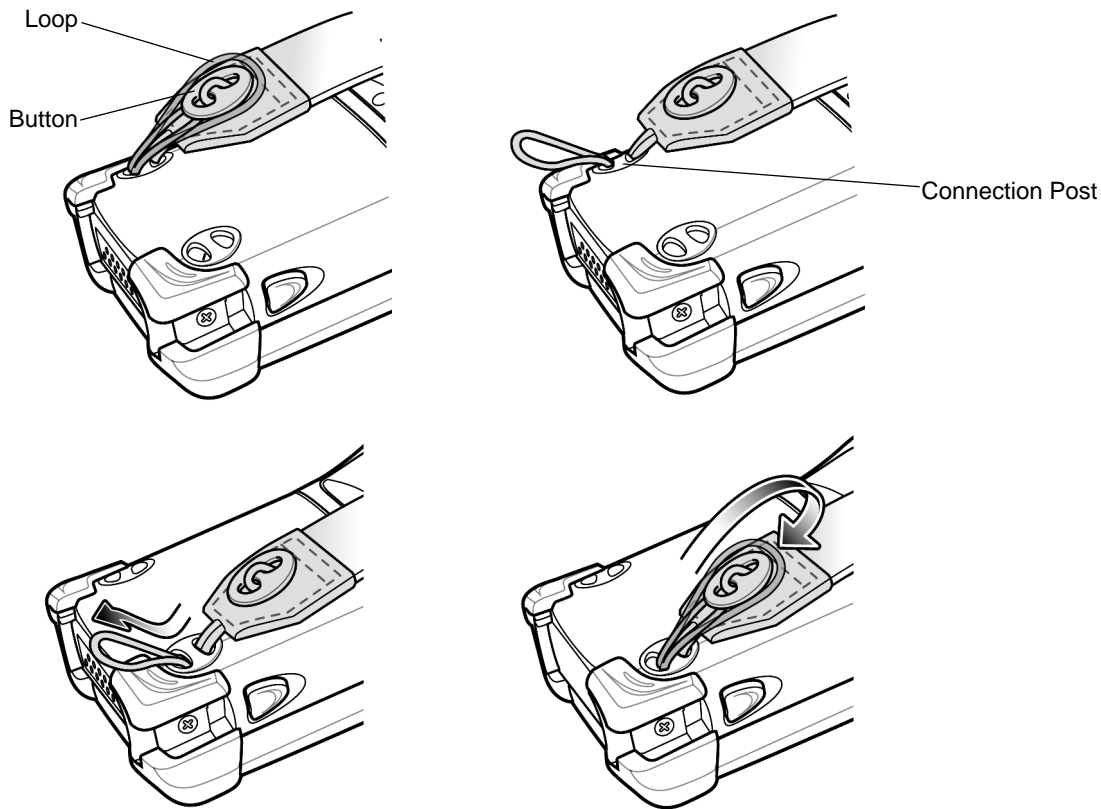
Figure 1-14 *Repositioning the MC909X-K Strap*

2. Pull the loop through the connection post.

3. Remove the battery.

4. Insert the loop into the opposite connection post.

5. Place the loop over the button and pull taught.

6. Replace the battery.

To replace the handstrap:

1. Remove two screws securing the strap bracket to the device.
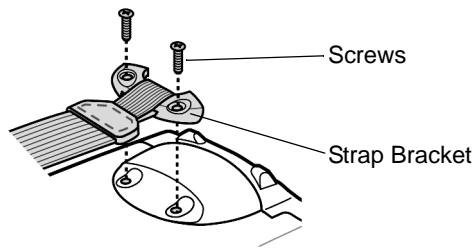
Figure 1-15   *Remove Strap Bracket*

2. Lift the loop end of the strap over the button.

3. Pull the loop through the connection post.

4. Remove the battery.

5. Reverse the procedure to re-attach the strap.

MC909X-S Strap

The strap may be moved to either the left or right side of the mobile computer to suit user preferences. To reposition the MC909X-S strap, attach the MC909X-S strap to either the left or right side of the mobile computer to suit user preferences. To reposition the strap:

1. Remove the screw securing the bottom of the strap to the device.

2. Position the bottom end of the strap over the opposite screw hole.

3. Secure the strap to the device.
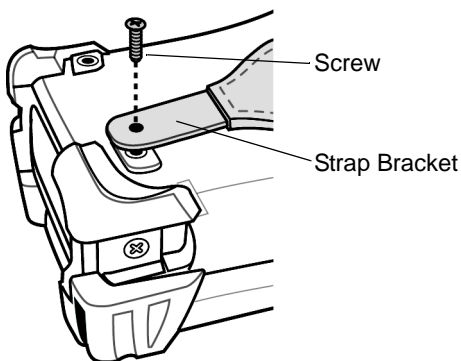
Figure 1-16   *Repositioning the MC909X-S Strap*

To replace the handstrap:

1. Remove two screws securing the strap bracket to the device.
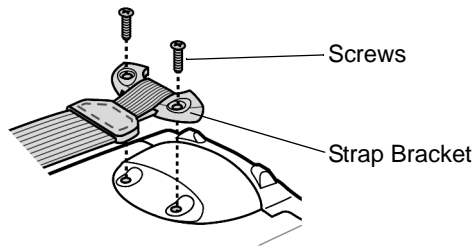
Figure 1-17   *Remove Strap Bracket*

2. Remove the screw securing the bottom of the strap to the device.

3. Reverse the procedure to re-attach the strap.

Battery Management

Battery Saving Tips

*   Leave the mobile computer connected to AC power at all times when not in use.

*   Set the mobile computer to turn off after a short period of non-use.

*   Set the display and keyboard backlight to turn off after a short period of non-use.

*   Turn off all wireless radio activity when not in use.

*   Power off the mobile computer when charging to charge at a faster rate.

Changing the Power Settings

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

1. On devices with Windows CE 5.0, tap **Start** > **Settings** > **Control Panel** > **Power** icon > **Power Off** tab.

    or

    On devices with Windows Mobile 5.0, tap **Start** > **Settings** > **System** tab > **Power** icon > **Advanced** tab.

2. Select the **On battery power: Turn off device if not used for:** check box and select a value from the drop-down list box.

3. Tap **OK**.

Changing the Display Backlight Settings

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

1. On devices with Windows CE 5.0, tap **Start** > **Settings** > **Control Panel** > **Backlight** icon > **Battery Power** tab.

   or

   On devices with Windows Mobile 5.0, tap **Start** > **Settings** > **System** tab > **Backlight** icon > **Battery Power** tab.

2. Select the **On battery power: Disable backlight if not used for:** check box and select a value from the drop-down list box.

3. Tap the **Brightness** tab.

4. Tap the **Disable backlight** check box to completely turn off the display backlight.

5. Use the slider to set the brightness of the backlight. Set it to a low value to save battery power.

6. Tap **OK**.

Changing the Keypad Backlight Settings

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

1. On devices with Windows CE 5.0, tap **Start** > **Settings** > **Control Panel** > **Keylight** icon > **Battery Power** tab.

   or

   On devices with Windows Mobile 5.0, tap **Start** > **Settings** > **System** tab > **Keylight** icon > **Battery Power** tab.

2. Select the **On battery power: Disable keylight if not used for:** check box and select a value from the drop-down list box.

3. Tap the **Advanced** tab.

4. Tap the **Disable keylight** check box to completely turn off the display backlight.

5. Tap **OK**.

Turning Off the Radios

On Devices with Mobile 5.0 AKU 1.0

NOTE   To determine the operating system AKU version, see *Software Versions on page xvii*.

Turning Off the WLAN Radio

To turn off the WLAN radio tap the **Wireless Connection Status** icon at the bottom of the Today screen and select **Disable Radio**. A red X appears across the icon indicating that the radio is disabled (off).

Wireless Connection Status Icon

Figure 1-18 *Wireless Connection Status Icon*

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

Bluetooth and WWAN Radios

> *NOTE* The Flight Mode feature only turns off the WWAN and Bluetooth radios. The WLAN radio must be turned off separately.

To turn off the Bluetooth and WWAN radios, tap the **Connectivity** icon (on non-WWAN devices) or the **Antenna/Signal** icon (on WWAN devices) and select **Turn On Flight Mode**.

> *NOTE* On the MC9097, it takes two to five seconds for the radio to shut down.

To turn on the Bluetooth and WWAN radios, tap the **Connectivity** icon (on non-WWAN devices) or the **Antenna/Signal** icon (on WWAN devices) and select **Turn Off Flight Mode**.

> *NOTE* On the MC9097, wait 20 to 40 seconds for the radio to power on. During this time do not suspend the mobile computer or remove the battery. If the mobile computer is suspended or the battery is removed, warm boot the mobile computer.

On Devices with Mobile 5.0 AKU 2.2 or higher

> *NOTE* To determine the operating system AKU version, see *Software Versions on page xvii*.

Windows Mobile 5.0 devices with AKU 2.2 or higher include **Wireless Manager**, which provides a simple method of enabling, disabling, and configuring all the device's wireless capabilities in one place.

To open **Wireless Manager**, tap the **Connectivity** icon.
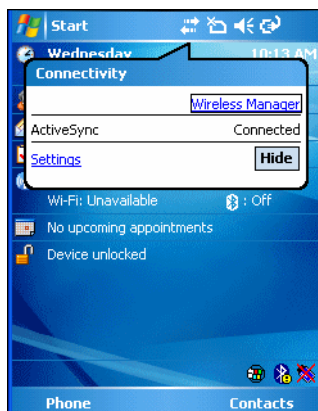
Figure 1-19 *Opening Wireless Manager*

Select **Wireless Manager**.
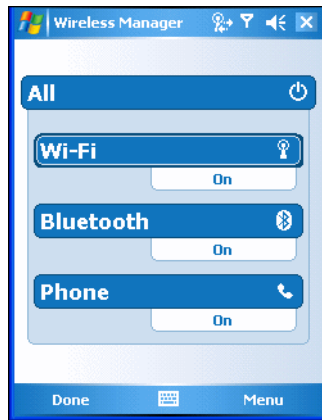
Figure 1-20   *Wireless Manager Window*

To enable or disable a wireless connection, tap its blue bar.

To enable or disable all wireless connections, tap and hold the **All** bar.

To configure settings for a connection, tap **Menu**.

Figure 1-21   *Wireless Manager Menu*

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

> **NOTE**   To determine the operating system OEM version, see *Software Versions on page xvii*.

WLAN Radio

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**.

Bluetooth Radio

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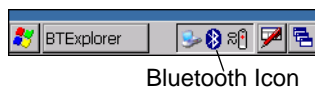
Bluetooth Icon

Figure 1-22 *Bluetooth Icon*

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

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

> **NOTE** To determine the operating system OEM version, see *Software Versions on page xvii*.

WLAN Radio

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).

Wireless Connection Status Icon
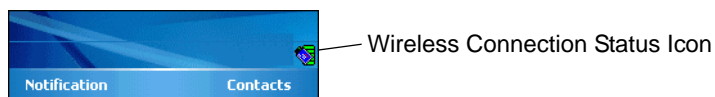
Figure 1-23 *Wireless Connection Status Icon*

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**.
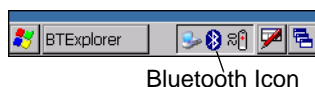
Bluetooth Icon

Figure 1-24 *Bluetooth Icon*

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

Chapter 2 Accessories

Introduction

Series 9000 accessories provide a wide variety of product support capabilities. Accessories include cradles, keypads, Magnetic Stripe Reader (MSR) and Cable Adapter Module (CAM) snap-on, four slot spare battery charger, headphone, Multimedia Card (MMC), Secure Device (SD) card, Universal Battery Charger (UBC) adapter, wall mounting bracket and shelf slide.

Keypads

- Optional keypads include the interchangeable modular application specific keypads listed below. The modular keypads can be changed in the field as necessary to support specialized applications.
- 28-key keypad
- 33-key keypad (MC909X-K only)
- 38-key Numeric keypad (MC909X-S only)
- 38-key Alpha keypad (MC909X-S only)
- 43-key keypad (MC909X-G and MC909X-K only)
- 53-key keypad (MC909X-G and MC909X-K only)
- 3270 Emulator keypad (MC909X-G and MC909X-K only)
- 5250 Emulator keypad (MC909X-G and MC909X-K only)
- VT Emulator keypad (MC909X-G and MC909X-K only).

Cradles

- Single Slot Serial/USB cradle charges the mobile computer main battery and 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 the mobile computer main battery.
- Four Slot Ethernet cradle charges the mobile computer main battery and synchronizes the mobile computer with a host computer through an Ethernet connection.

Miscellaneous

- Four Slot Spare Battery Charger charges up to four mobile computer spare batteries.

- Headphone can be used in noisy environments.

- Modem Module enables data communication between the mobile computer and a host computer, remotely through the phone lines, and synchronizes information between the mobile computer and a host computer.

- Multimedia Card (MMC) provides secondary non-volatile storage. (An SD card may also be used.)

- UBC adapter charges spare batteries.

- Wall Mounting Bracket and Shelf Slide can be used for wall mounting applications.

Snap-on Modules

- MSR connects on to the mobile computer and adds magstripe read capabilities.

- CAM connects on to the mobile computer and is used to connect cables to the mobile computer.

Both of the snap-on modules use the cables listed below:

- AC line cord (country-specific) and power supply, charges the mobile computer.

- Auto charge cable, charges the mobile computer using a vehicle's cigarette lighter.

- DEX cable, connects the mobile computer to a vending machine.

- Serial cable, adds serial communication capabilities.

- USB cable, adds USB communication capabilities.

- Printer cable, adds printer communication capabilities.

Keypads

The mobile computer has interchangeable modular keypads. The modular keypads can be changed in the field as necessary to support specialized applications.

✓ **NOTE** Do not remove the keypad while the mobile computer is on and do not operate the mobile computer with the keypad detached. Follow proper Electro-Static Discharge (ESD) precautions to avoid damaging the MMC and SD card. Proper ESD precautions include, but are not limited to, working on an ESD mat and ensuring that the operator is properly grounded.

MC9090 keypads are not interchangeable with MC9060 keypads.

Replacing the Keypad

1. Press the **Power** button to suspend the mobile computer.

2. Remove the two keypad screws. Slide the keypad down and lift up.
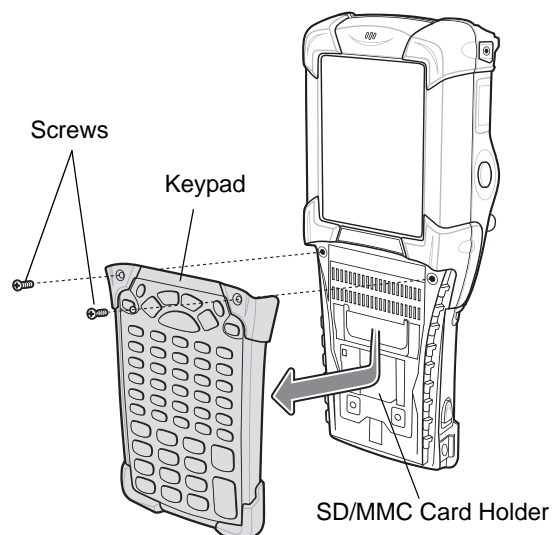
Figure 2-1   *Removing the Keypad*

⚠️ **CAUTION**   Do not apply more than 4 in-lbs of torque when tightening the keypad screws.

3.   Replace the keypad and re-attach using the two screws.
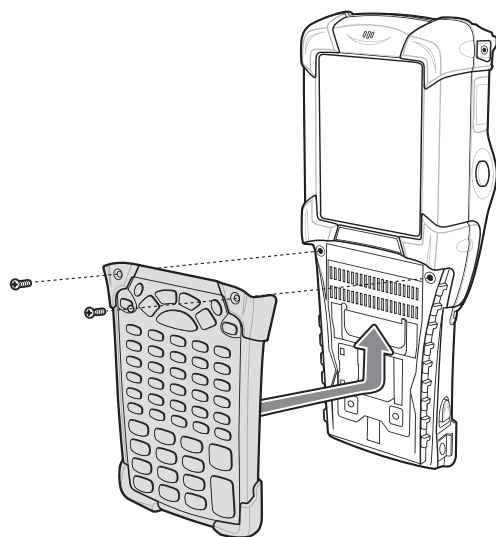
Figure 2-2   *Installing the Keypad*

4.   Perform a warm boot.

Multi Media Card (MMC) / Secure Device (SD) Card

The MMC provides secondary non-volatile storage. The MMC is located under the keypad (see *Figure 2-1*).

NOTE   SD cards are inter-operable with MMC cards and can also be used in MC909X mobile computers.

MC909X with Windows Mobile 5.0 with OEM Version 01.39.0001
MC909X with Windows CE 5.0 with OEM Version 01.26.0001.

CAUTION   Do not remove the keypad while the mobile computer is on and do not operate the mobile computer with the keypad detached. Follow proper ESD precautions to avoid damaging the MMC/SD. Proper ESD precautions include, but are not limited to, working on an ESD mat and ensuring that the operator is properly grounded.

To insert the MMC/SD card:

1.   Press the **Power** button to suspend the mobile computer.

2.   Remove the two keypad screws and slide the keypad down and lift off (see *Figure 2-1 on page 2-3*).

3.   Lift the MMC/SD retaining door.

4.   Position the MMC/SD card, with the contacts down, into the MMC/SD holder. The MMC/SD card corner notch fits into the holder only one way.

5.   Snap the retaining door closed.

MMC/SD

MMC/SD Retaining Door
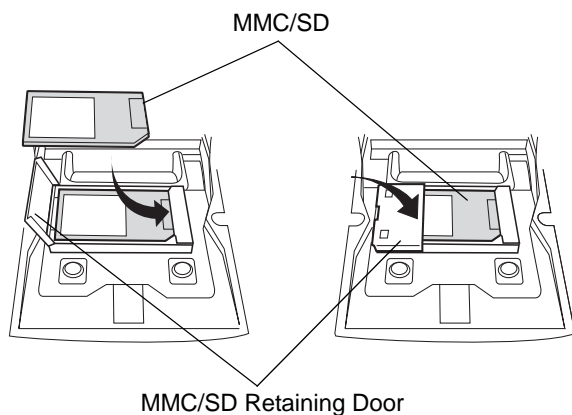
Figure 2-3   *Inserting the MMC/SD*

CAUTION   Do not apply more than 4 in-lbs of torque when tightening the keypad screws.

6.   Replace the keypad and re-attach using the two screws (see *Figure 2-2 on page 2-3*).

7.   Perform a warm boot.

Single Slot Serial/USB Cradle

⚠️ **CAUTION**   Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 10-1*.

This section describes how to set up and use a single Single Slot Serial/USB cradle with the mobile computer. For serial and USB communication setup procedures see *Serial Communication Setup on page 2-44*.
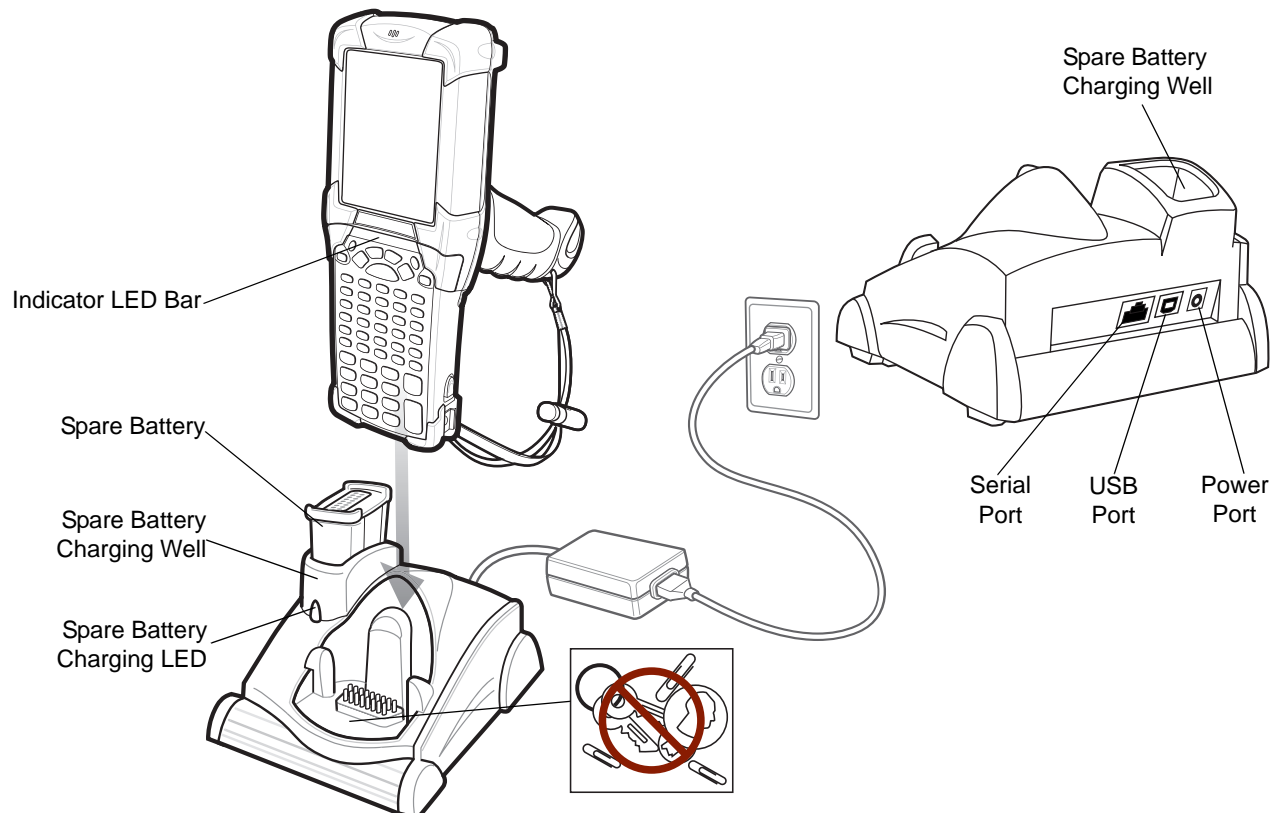
Figure 2-4   *Single Slot Serial/USB Cradle*

⚠️ **CAUTION**   Do not place coins, keys or paper clips in cradle well.

The Single Slot Serial/USB Cradle:

- Provides 15VDC power for operating the mobile computer.

- Provides serial and USB ports for data communication between the mobile computer and a host computer or other serial devices (e.g., a printer).

    ✓ **NOTE**   When a mobile computer with Microsoft Mobile 5.0 is placed in the cradle 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.

- Synchronizes information between the mobile computer and a host computer. (With customized or third party software, it can also be used to synchronize the mobile computer with corporate databases.)

- Charges the mobile computer's battery.

- Charges a spare battery.

MC909X-S Battery

Short Battery Adapter
(P/N BAP9000-100)

Spare Battery
Charging Well
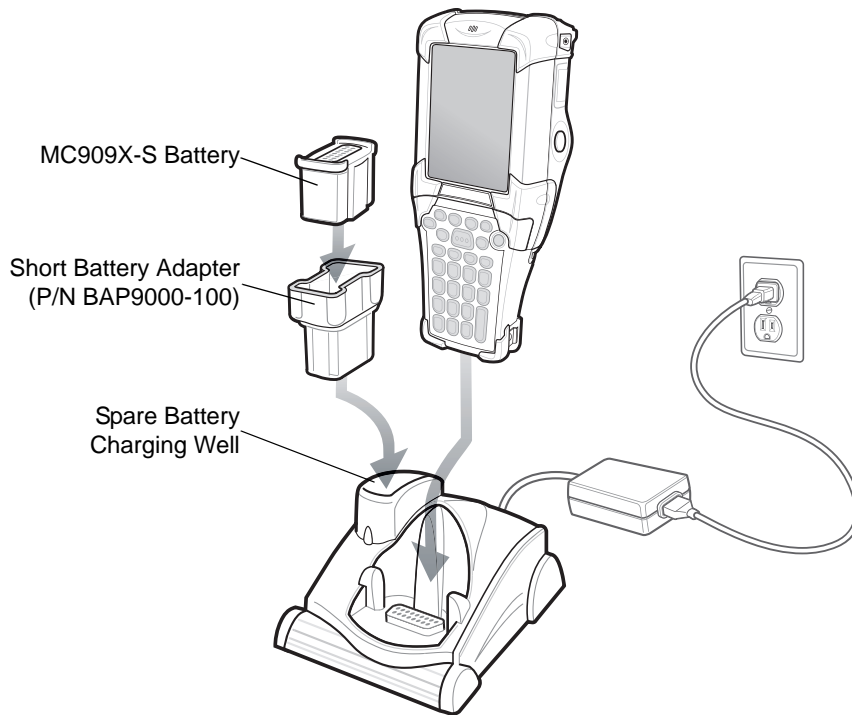
Figure 2-5   *MC909X-S Spare Battery Charging*

Setup

⚠ **CAUTION**   Use only a Symbol approved power supply output rated 12 VDC and minimum 3.3 A. Use of an alternative power supply will void the product warranty and may cause product damage. Refer to the *MC909X User Guide* for the power supply regulatory compliance statement.

✓ **NOTE**   The cradle requires a dedicated port on the host. Select either serial or USB for communications. Do not connect the cradle to both serial and USB ports.
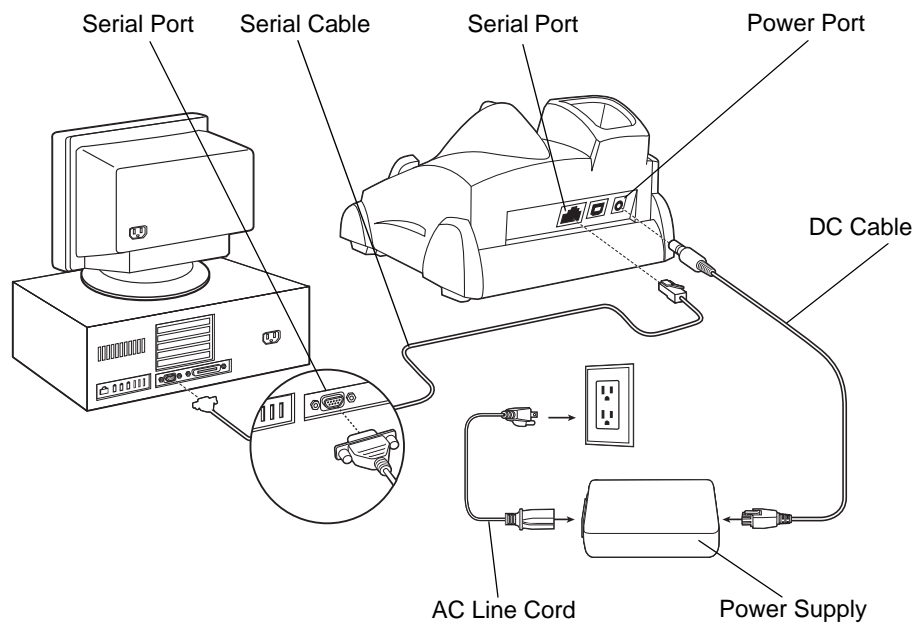
Figure 2-6   *Single Slot Cradle Power/Serial Connections*
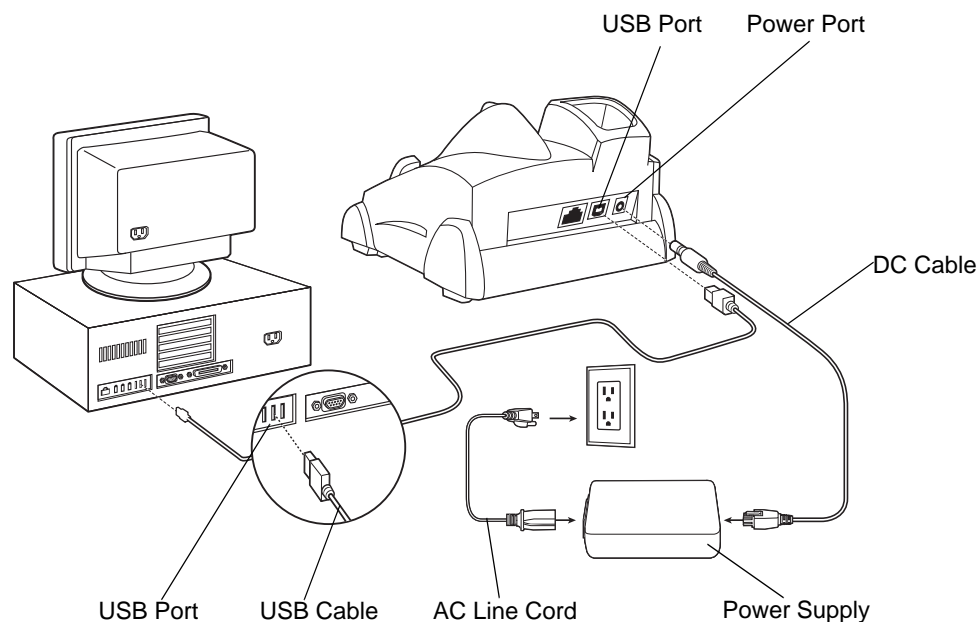
Figure 2-7   *Single Slot Cradle Power/USB Connections*

Battery Charging Indicators

The Single Slot Serial/USB Cradle can charge the mobile computer's main battery and a spare battery simultaneously. The mobile computer's amber charge LED, located in the Indicator LED Bar, shows the status of the battery charging in the mobile computer. See *Table 1-2 on page 1-8* for charging status indications. The amber spare battery charging LED on the cradle (see *Figure 2-4 on page 2-5*) shows the status of the spare battery charging in the cradle. See *Table 2-1* for charging status indications. Batteries usually charge in less than four hours.

Table 2-1   *Spare Battery LED Charging Indicators*

Spare Battery LED (on cradle)	Indication
Off	No spare battery in well; 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.

Four Slot Ethernet Cradle

⚠️ **CAUTION** Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 10-1*.

This section describes how to set up and use a Four Slot Ethernet cradle with the mobile computer. For cradle communication setup procedures see *Ethernet Communication Setup on page 2-11*.
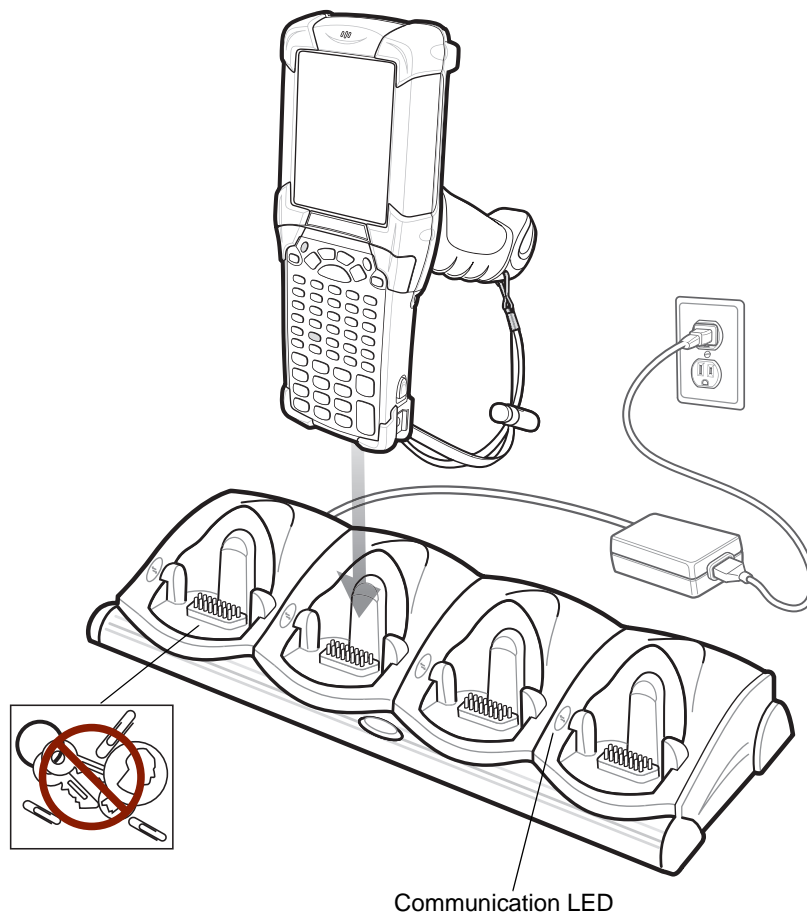
Communication LED

Figure 2-8   *Four Slot Ethernet Cradle*

⚠️ **CAUTION** Do not place coins, keys or paper clips in cradle well.

The Four Slot Ethernet cradle:

- Provides 12VDC power for operating the mobile computer.

- Enables data communication between the mobile computer (up to four) and a host computer, over an Ethernet network (using a standard 10Base-T Ethernet cable).

- Synchronizes information between the mobile computer and a host computer. (With customized or third party software, it can also be used to synchronize the mobile computer with corporate databases.)

- Simultaneously charges up to four batteries in the mobile computer.

Table 2-2   *Communication LED*

Status	Indication
Off	Mobile computer is not in cradle; mobile computer not placed correctly; cradle is not powered.
Solid Red	Mobile computer is present, but communication has not started.
Flashing Green	Mobile computer is in the cradle, and communicating with the host computer.
Slow Flashing Red	Error, communication did not start.
Fast Flashing Red	Warning: Terminal inactivity time-out. The terminal did not finish data synchronization or had an open connection for more than 15 minutes. This time is programmable in the cradle flash parameters.
Solid Green	Terminal is present in the slot and communication is complete.
All LEDs Flashing Red	Failed automatic cradle configuration via local DHCP Service.

Setup

⚠️ **CAUTION**   Use only a Symbol 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. Refer to the *MC909X User Guide* for the power supply regulatory compliance statement.

✓ **NOTE**   The Four Slot Ethernet cradle must be connected to a power source and to an Ethernet Hub (when applicable).

Figure 2-9   *Four Slot Ethernet Cradle Power Connection*

Battery Charging Indicators

The mobile computer's amber charge LED, located in the Indicator LED Bar, shows the status of the battery charging in the mobile computer. See *Table 1-2 on page 1-8* for charging status indications. The battery usually charges in less than four hours.

Ethernet Communication Setup

To establish a connection between the mobile computer and the host computer to communicate over an Ethernet network, perform the following:

- Install MobileDox Cradle Manager
- Install iDockIt
- Configure the mobile computer
- Configure the host computer
- Configure the DHCP server
- Configure the cradle.

Installing MobileDox Cradle Manager

NOTE   MobileDox Cradle Manager is used only when establishing a connection using the Four Slot Ethernet cradle.

The Cradle Management software features:

- View cradles that are attached to the network via MobileDox Net
- View cradle status
- Modify cradle settings including:
  - IP address settings
  - DNS and WINS settings
  - Identification settings
  - USB port specific settings
- Restart cradles connected to the network via MobileDox Net
  Update the firmware of MobileDox Net.

To install the Cradle Management Software on the host computer, download the latest version of the software from http://support.symbol.com. Refer to the instructions included with the software.

Installing iDockIt

iDockIt is a connection utility which manages activities between the mobile computer and a connected Ethernet cradle. For more information on the utility, see the documentation provided with *iDockIt*.

iDockIt features:

- The ability to manage multiple cradle profiles. *iDockIt* auto-detects the cradle communication type and behaves accordingly.
- Integrated modem capabilities using TAPI interface.

- Runs as a tray application, and always runs in the background.

- The ability to configure settings within the application.

- Options to change parameters upon docking (with or without settings time-out).

- The ability to force synchronization events.

- The ability to disable WLAN connection on the device to ensure synchronization is performed via dock.

- Management of multiple connection types without losing settings.

On MC909X mobile computers with Windows CE 5.0 or with Windows Mobile 5.0 and OEM version lower than 28, the *iDockIt* installation file is To install *iDockIt* on the mobile computer download the latest version of the *iDockIt* software from http://support.symbol.com to the host computer. Follow the instructions provided with the *iDockIt* software to install *iDockIt* onto the mobile computer.

On MC909X mobile computers with OEM version 28 and higher, the *iDockIt* installation file is loaded on the mobile computer. To install *iDockIt*:

1. Open **File Explorer**.

2. Navigate to the **Application** directory.

3. Tap the file: *IDOCKIT_4.02.05.2_MC90XX_WM5.cab*

iDockIt installs on the mobile computer. Follow the onscreen instruction.

Refer to *Appendix B, Using iDockIt* for instructions on configuring and using iDockIt.

Mobile Computer Configuration

Inserting the mobile computer into the cradle provides direct-connect Remote Access Service (RAS) service. Configure each mobile computer for use with the cradle, just as any remote client would be configured to connect to an Internet Service Provider (ISP). The computer comm port setting was set to USB during the iDockIt installation procedure.

DHCP Server Configuration

If you use a DHCP server to distribute IP addresses and other network parameters, the server setup should include the following:

- IP address pool (1 or 5 IP address per cradle)

- Router/gateway address

- One or more DNS server addresses

- One or more WINS server addresses

- Subnet mask.

NOTE   To assign the initial cradle IP address, you can either use a DHCP server, as shown above, or use the MobileDox Cradle Manager (see *Installing MobileDox Cradle Manager on page 2-11*). The DHCP server is the preferred method.

Cradle Configuration

The MobileDox Cradle Manager allows you to setup the Device IP Address and modify cradle settings. See *Installing MobileDox Cradle Manager on page 2-11* for instructions to download and install the software. See *Figure 2-8 on page 2-9* for instructions on Four Slot Ethernet cradle connections.

Setting the Device IP Address

By default, the cradle uses DHCP to obtain its IP address. However, if DHCP fails, the Cradle Manager can assign an IP address.

> **NOTE** This is used if the cradle is connected to the network, but fails to appear in MobileDox. Enter the hardware device (MAC) address to locate the cradle and assign it a new IP address.

To set the IP address:

1. Launch the MobileDox Cradle Manager on the host computer.

2. Click **File** > **Set IP Address of Unlisted Device**. The Set IP Address window appears:

Figure 2-10 *Set IP Address Window*

3. Enter the appropriate MAC Address and IP address.

4. Click **OK**.

Modifying Cradle Settings

1. Launch the MobileDox Cradle Manager on the host computer.

2. Select the name of the cradle you want to configure from the list.

3. Click **Device** > **Modify Settings**.

4. Use the **General Settings** tab to modify the identification settings of the cradle.
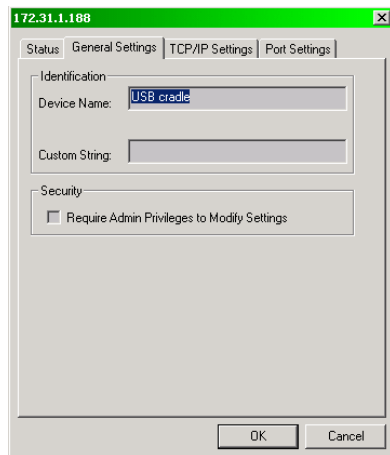
Figure 2-11   *Cradle Settings Window - General Settings Tab*

Table 2-3   *Cradle Settings - General Settings Fields*

Field	Description
Device Name	A text string used to describe the MobileDox device. Any 15-character string may be entered.
Custom String	A text string for any desired usage (examples are: location, asset ID, etc.). Any 15-character string may be entered.
Require Admin Privileges to Modify Settings check box	Selecting this check box requires users to have administrative privileges in order to modify MobileDox settings. Administrative privileges are validated using standard Windows authentication.

5.   Use the **TPC/IP Settings** tab to modify the DNS and WINS identification settings of the cradle.
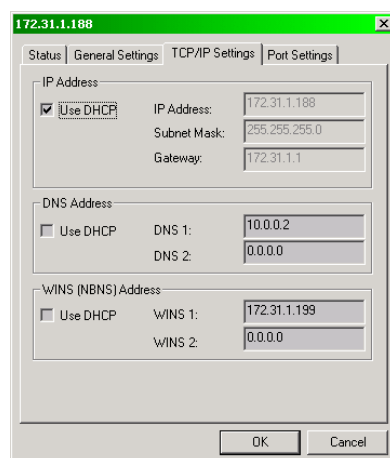
Figure 2-12   *Cradle Settings Window - TCP/IP Settings Tab*

Table 2-4 *Cradle Settings - TCP/IP Settings Fields*

Field	Description
Use DHCP	If check box is selected, necessary information is retrieved from the DHCP server. If check box is not selected, static configuration is used (information needs to be entered).
IP Address	The IP address that the MobileDox uses when communicating on the network.
Subnet Mask	The subnet mask that the MobileDox uses when communicating on the network.
Gateway Address	The IP address that the MobileDox uses to send non-local IP network data.
DNS Address	The IP address of a server(s) that can resolve Internet names into IP addresses.
WINS Address	The IP address of a server(s) that can resolve Windows network names into IP addresses. This field must be populated correctly when using ActiveSync.

6.   Use the **Port Settings** tab to modify the USB port settings of the cradle.
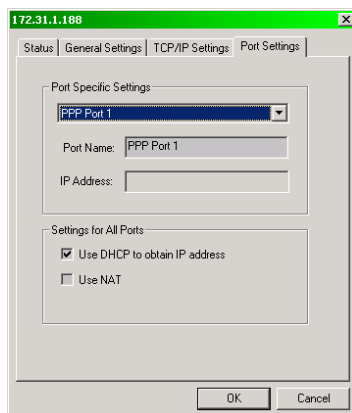
Figure 2-13 *Cradle Settings Window - Port Settings Tab*

Table 2-5 *Cradle Settings - Port Settings Fields*

| Field	Description
Port Name	A text string used to describe the device attached to the port. Any 15-character string can be entered. You can specify up to four port names, one for each of the cradle's slots.
IP Address	The IP address assigned to the cradled device. There should be one IP address per cradle slot. This box is disabled for all devices if DHCP is used to obtain the IP address.
Use DHCP to obtain IP Address check box	The cradle uses DHCP to obtain an IP address for the handheld. Unchecking this selection allows the cradle to use Static IP address for the handheld.
Use NAT check box	The cradle uses Network Address Translation (NAT) when forwarding handheld traffic onto the network. No IP addresses are necessary for the handhelds. This must be disable when using ActiveSync.

7.   Click **OK**.

Four Slot Charge Only Cradle

⚠️ **CAUTION** Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 10-1*.

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


Figure 2-14 *Four Slot Charge Only Cradle*

⚠️ **CAUTION** Do not place coins, keys or paper clips in cradle well.

The Four Slot Charge Only cradle:

- Provides 12VDC power for operating the mobile computer.
- Simultaneously charges up to four batteries in the mobile computer.

Setup

| ⚠ | *CAUTION* | Use only a Symbol 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. Refer to the *MC909X User Guide* for the power supply regulatory compliance statement. |
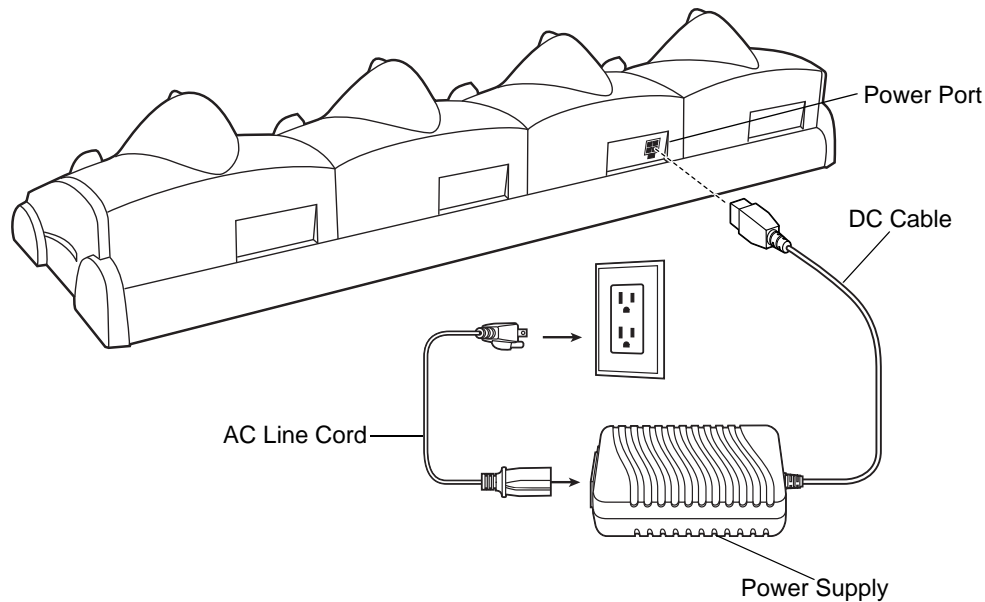
Figure 2-15   *Four Slot Charge Only Cradle Power Connection*

Battery Charging Indicators

The mobile computer's amber charge LED, located in the Indicator LED Bar, shows the status of the battery charging in the mobile computer. See *Table 1-2 on page 1-8* for charging status indications. The battery usually charges in less than four hours.

Four Slot Spare Battery Charger

⚠️ **CAUTION**   Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 10-1*.

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

MC909X-S Battery

Short Battery Adapter

Spare MC909X-G/K Battery

Spare Battery Charging LEDs (4)

Spare Battery Charging Well (4)
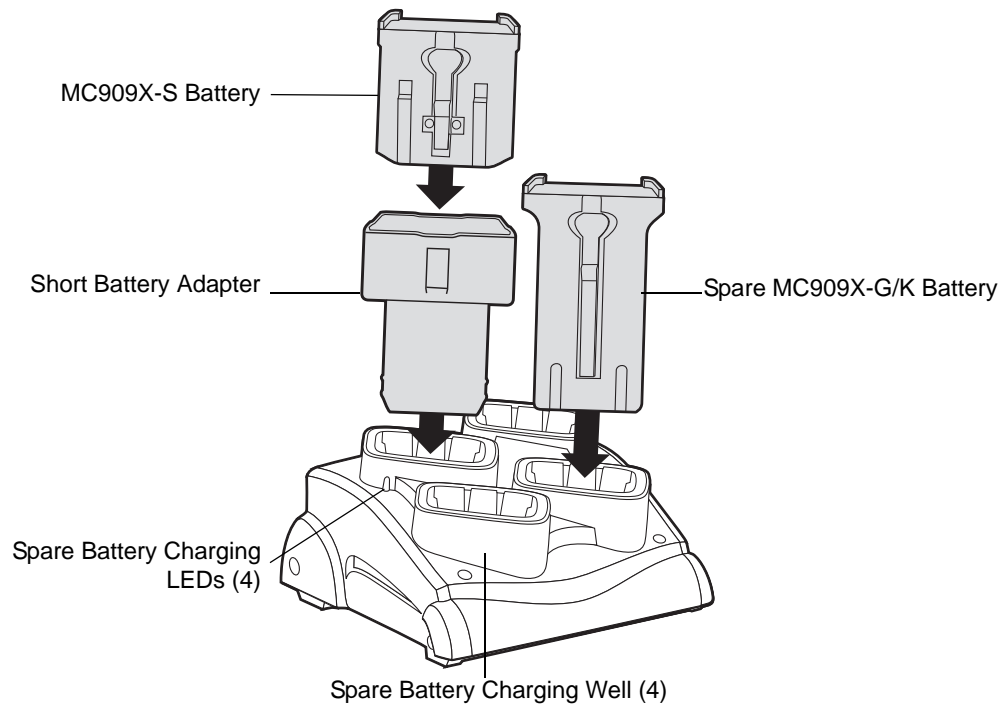
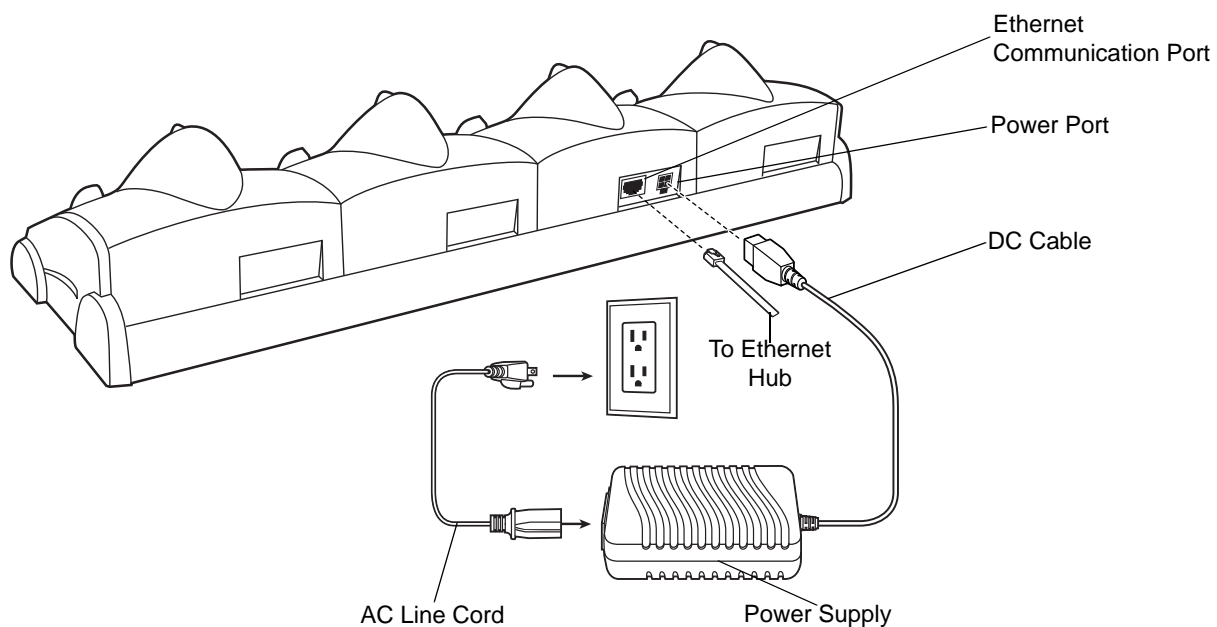**Figure 2-16**   *Four Slot Spare Battery Charger*

Setup

| ⚠ | **CAUTION** | Use only a Symbol approved power supply output rated 15 VDC and minimum 5 A. Use of an alternative power supply will void the product warranty and may cause product damage. Refer to the *MC909X User Guide* for the power supply regulatory compliance statement. |

Power Port

DC Cable

AC Cord

Power Supply
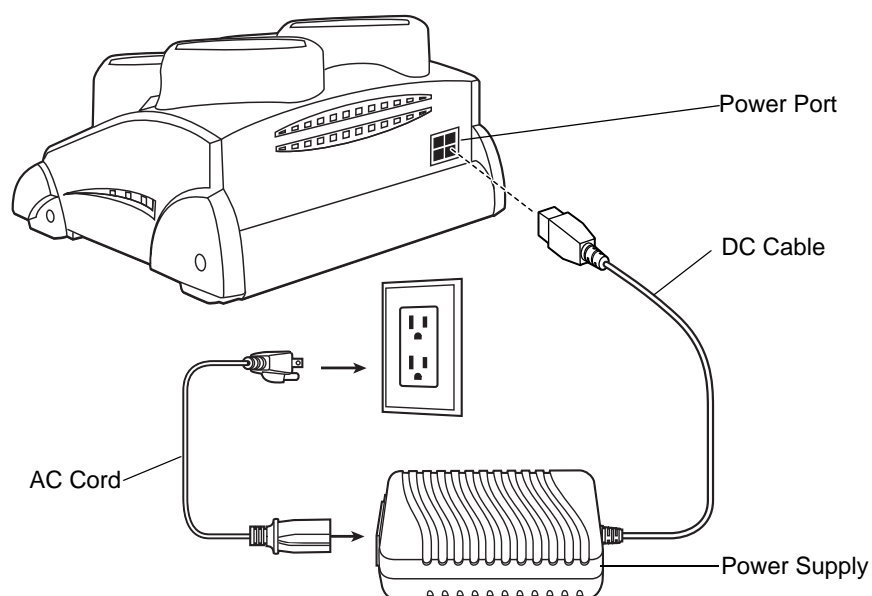
Figure 2-17   *Four Slot Spare Battery Charger Power Connection*

Spare Battery Charging with the Four Slot Spare Battery Charger

1. Connect the charger to a power source as shown in *Figure 2-17*.

2. Insert the battery into a spare battery charging slot and gently press down on the battery to ensure proper contact.

Battery Charging Indicators

An amber LED is provided on each battery charging well (see *Figure 2-16 on page 2-18*). See *Table 2-6* for charging status indications.

The battery usually charges in less than four hours.

Table 2-6   *Spare Battery LED Charging Indicators*

LED	Indication
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.

Magnetic Stripe Reader

This section describes how to set up and use the snap-on MSR with the mobile computer. The MSR snaps on to the bottom of the mobile computer and can be easily removed when not in use.
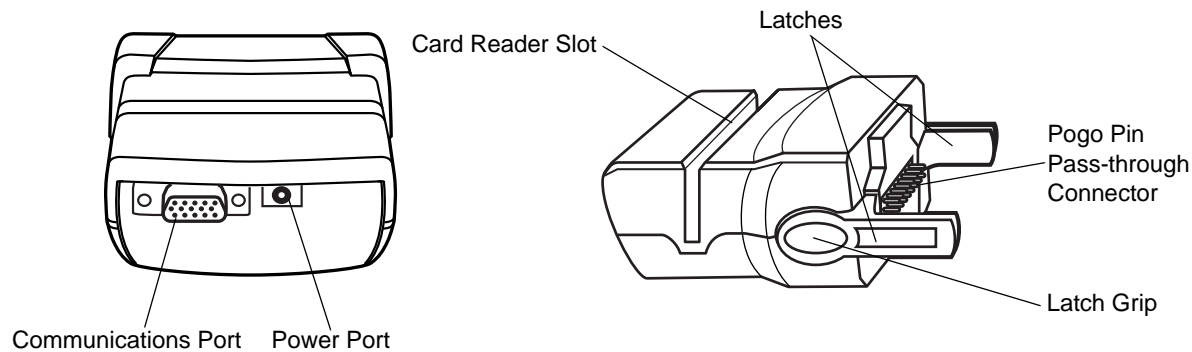
Figure 2-18   *Magnetic Stripe Reader*

When attached to the mobile computer, the MSR:

- Provides power for operating the mobile computer, with the appropriate power connection.

- Allows the mobile computer to capture data from magnetic stripe cards. (To download MSR data capture software, visit: http://support.symbol.com.)

NOTE When a mobile computer with Windows Mobile 5.0 is connected to a host computer through the MSR 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.

- 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 2-44*.

- 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 *Serial Communication Setup on page 2-44*.

- Charges the mobile computer's battery, when used with the appropriate power supply.

Attaching and Removing

To attach, snap the MSR onto the bottom of the mobile computer.

Latch Grip
(one on each side)
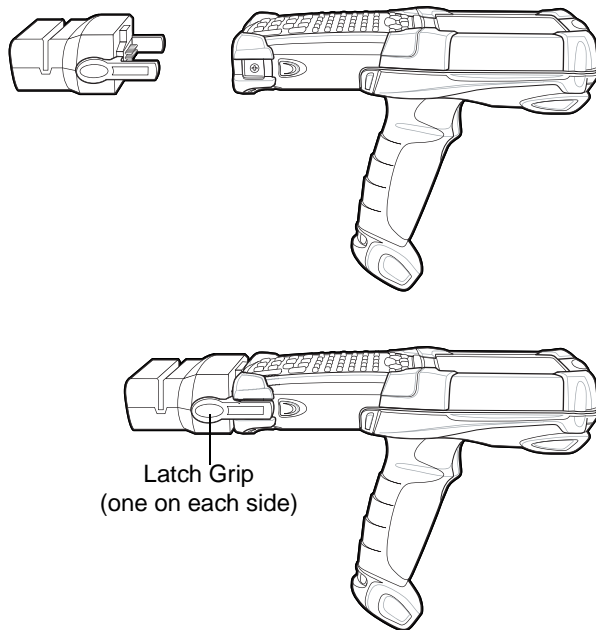
Figure 2-19   *Attaching the MSR*

To remove, squeeze the latch grips and pull the MSR from the mobile computer.

NOTE   Remove the MSR from the bottom of the mobile computer before using a cradle for charging and communication.

Setup

CAUTION   Use only a Symbol approved power supply output rated 12 VDC and minimum 3.3 A. Use of an alternative power supply will void the product warranty and may cause product damage. Refer to the *MC909X User Guide* for the power supply regulatory compliance statement.

AC Power Supply

Vehicle Power Supply

Into Cigarette Lighter
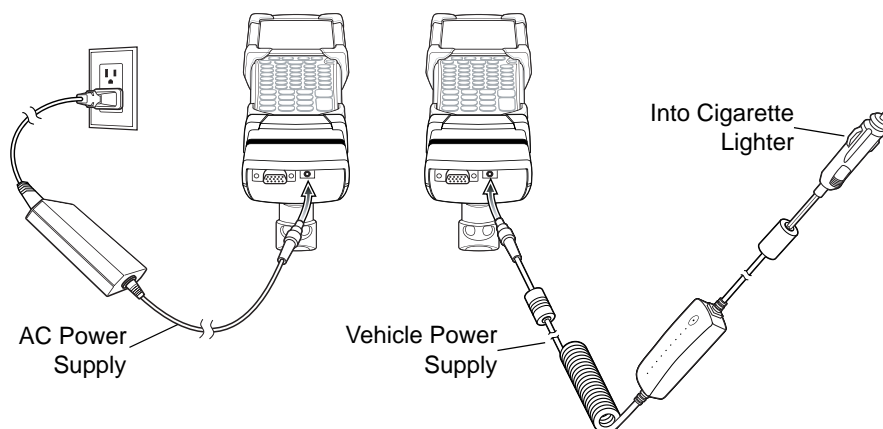
Figure 2-20   *MSR Power Connection*
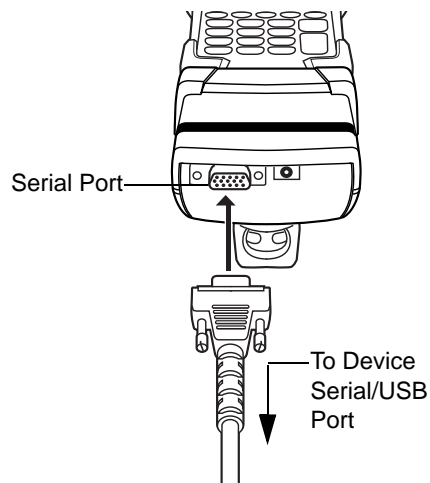
Figure 2-21   *MSR Serial/USB Connection*

Battery Charging Indicators

To charge the mobile computer's battery through the MSR, connect the power supply to the MSR (see *Figure 2-20 on page 2-21*), then attach the MSR to the mobile computer. The mobile computer begins charging automatically.

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

The mobile computer's amber charge LED, located in the Indicator LED Bar, shows the status of the battery charging in the mobile computer. See *Table 1-2 on page 1-8* for charging status indications.

The battery usually charges in less than four hours, if the mobile computer is not in use.

Serial/USB Connection

The MSR can connect to and communicate with a serial/USB device, such as a printer or host computer, through its serial port. See *Serial Communication Setup on page 2-44* for the host computer communication setup procedure.

To connect the MSR to a serial/USB device, connect one end of the serial device cable into the serial port on the MSR and the other end into the serial/USB port on the device.

Using the MSR

The *MSR9000* sample application is designed to work with the MSR. This sample application illustrates how an application should handle MSR inputs (refer to the *Symbol Application Guide for Symbol Devices*).

> *NOTE*   The MSR does not need to be attached to the power supply to read magnetic stripes.

To use the MSR:

1. Attach the MSR to the mobile computer (see *Attaching and Removing on page 2-21*).

2. Power on the mobile computer.

3. Tap **Start** > **9000 Demo** > **Test Apps** > **MSR 9000** or **MSR Cameo** to start the sample application.

4. Swipe the magnetic stripe card through the MSR, ensuring the magnetic stripe on the card faces the mobile computer. The card may be swiped in either direction, from left to right or from right to left. For best results, gently press down on the card while swiping to ensure contact with the bottom of the reader.
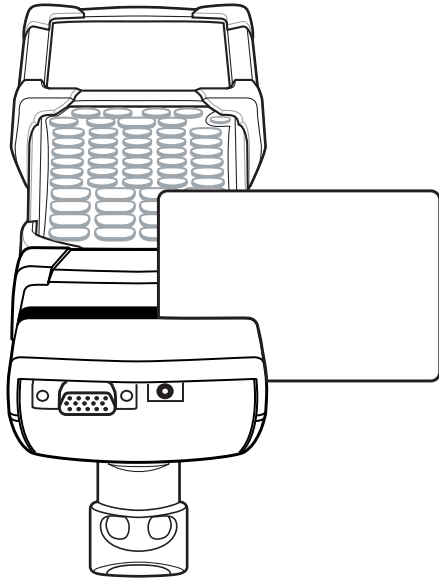
Figure 2-22   *Magnetic Stripe Card Swiping*

Cable Adapter Module

This section describes how to set up and use the snap-on CAM with the mobile computer. The CAM snaps on to the bottom of the mobile computer and can be easily removed when not in use.

Latches

Pogo Pin Pass-through Connector

Latch Grip

Communications Port   Power Port
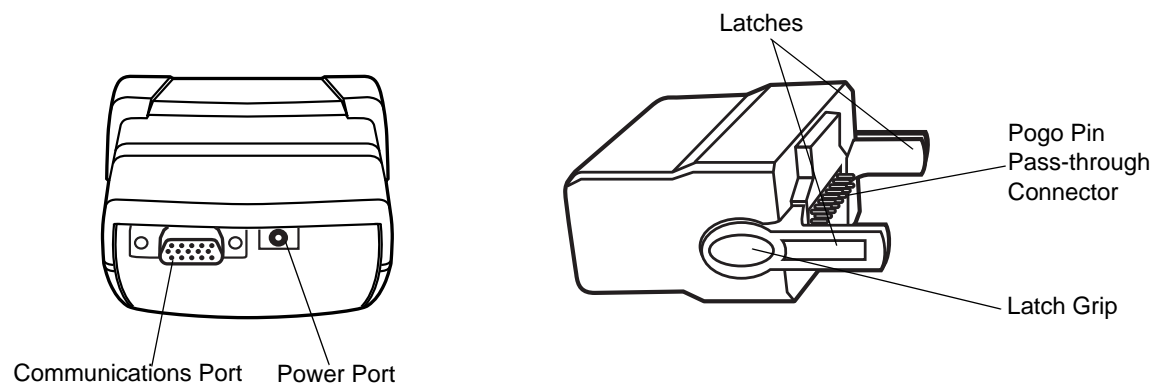
Figure 2-23   *Cable Adapter Module*

When attached to the mobile computer, the CAM:

- Provides power for operating the mobile computer, with the appropriate power connection.

    NOTE   When a mobile computer with Windows Mobile 5.0 is connected to a host computer through the CAM 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.

- 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 2-44*.

- 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 *Serial Communication Setup on page 2-44*.

- Charges the mobile computer's battery, when used with the appropriate power supply.

Attaching and Removing

To attach, snap the CAM onto the bottom of the mobile computer.

Latch Grip
(one on each side)
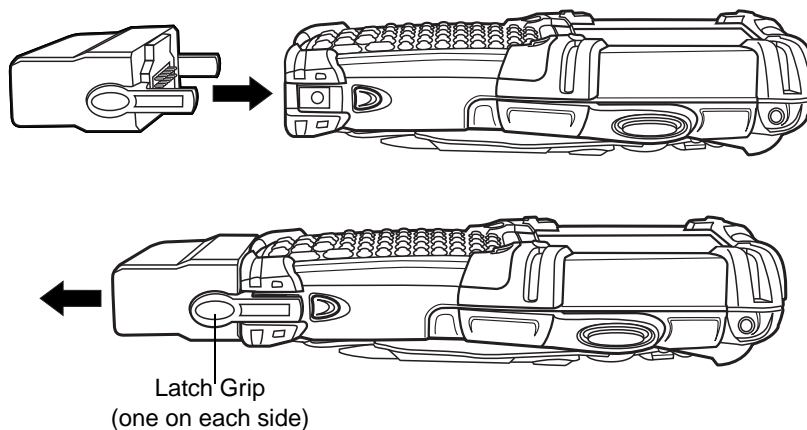
Figure 2-24   *Attaching the CAM (MC909X-K shown)*

To remove, squeeze the latch grips and pull the CAM from the mobile computer.

NOTE   Remove the CAM from the bottom of the mobile computer before using a cradle for charging and communication.

Setup

CAUTION   Use only a Symbol approved power supply output rated 12 VDC and minimum 3.3 A. Use of an alternative power supply will void the product warranty and may cause product damage. Refer to the *MC909X User Guide* for the power supply regulatory compliance statement.

OR

Into Cigarette
Lighter

AC Power
Supply

Vehicle Power
Supply
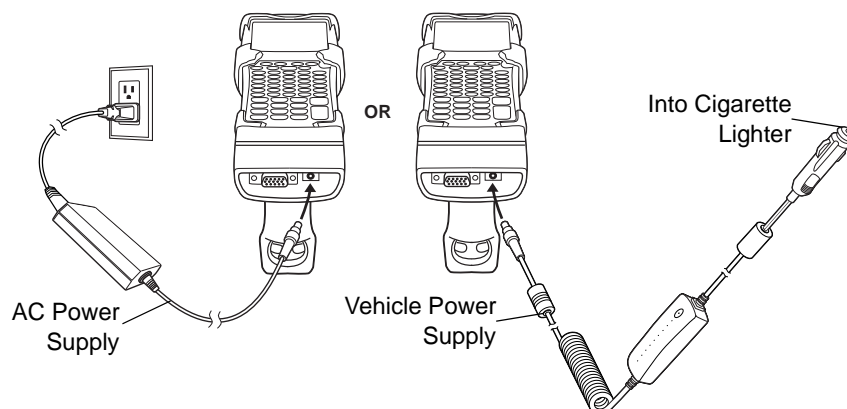
Figure 2-25   *CAM Power Connection*
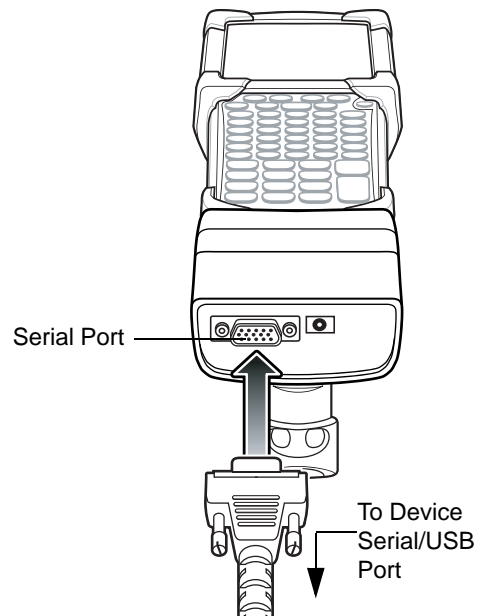
Figure 2-26   *CAM Serial Connection*

Battery Charging Indicators

To charge the mobile computer's battery through the CAM, connect the power supply to the CAM (see *Figure 2-25 on page 2-24*), then attach the CAM to the mobile computer. The mobile computer begins charging automatically.

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

The mobile computer's amber charge LED, located in the Indicator LED Bar, shows the status of the battery charging in the mobile computer. See *Table 1-2 on page 1-8* for charging status indications. The battery usually charges in less than four hours, if the mobile computer is not in use.

Serial/USB Connection

The CAM can connect to and communicate with a serial/USB device, such as a printer or host computer, through its serial port. See *Serial Communication Setup on page 2-44* for the host computer communication setup procedure.

To connect the CAM to a serial/USB device, connect one end of the serial device cable into the serial port on the CAM and the other end into the serial/USB port on the device.

Universal Battery Charger (UBC) Adapter

⚠️ **CAUTION** Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 10-1*.

This section describes how to use the UBC adapter to charge a spare battery.

The UBC can be used with a power supply as a standalone spare battery charger or it can be used with the four station UBC2000 to provide charging to simultaneously charge up to four spare batteries. For additional information about the UBC2000, see the *UBC 2000 Universal Battery Charger Product Guide* (p/n 70-33188-xx)
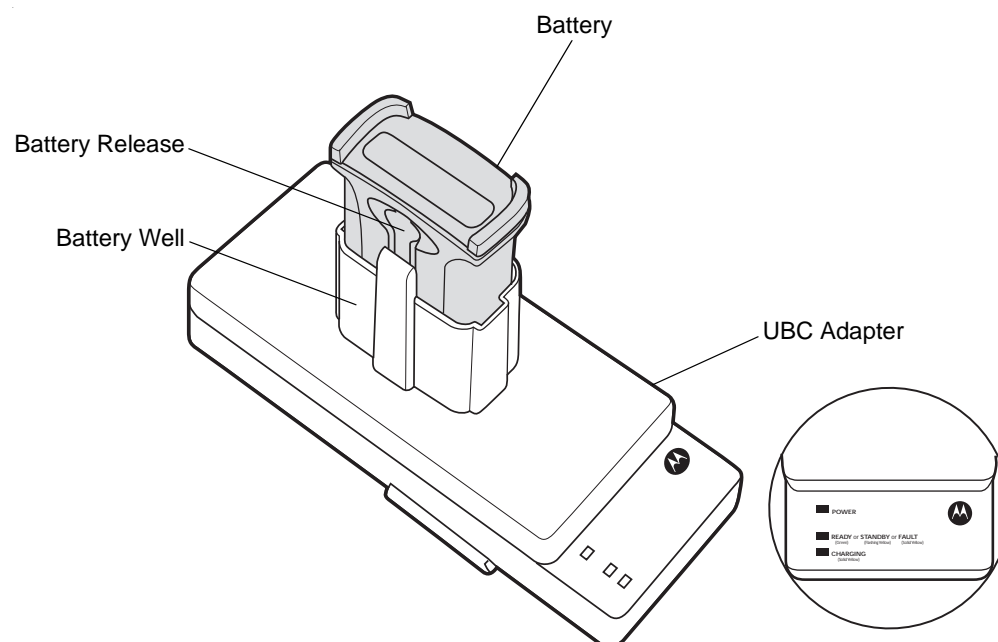
Figure 2-27   *UBC Adapter*

Inserting and Removing a Battery

Insert the battery into the battery well with the charging contacts facing down (over charging pins) and gently press down on the battery to ensure proper contact.

To remove the battery, press the battery release and lift battery out of the well.

Setup

⚠️ **CAUTION** Use only a Symbol 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. Refer to the *MC909X User Guide* for the power supply regulatory compliance statement.
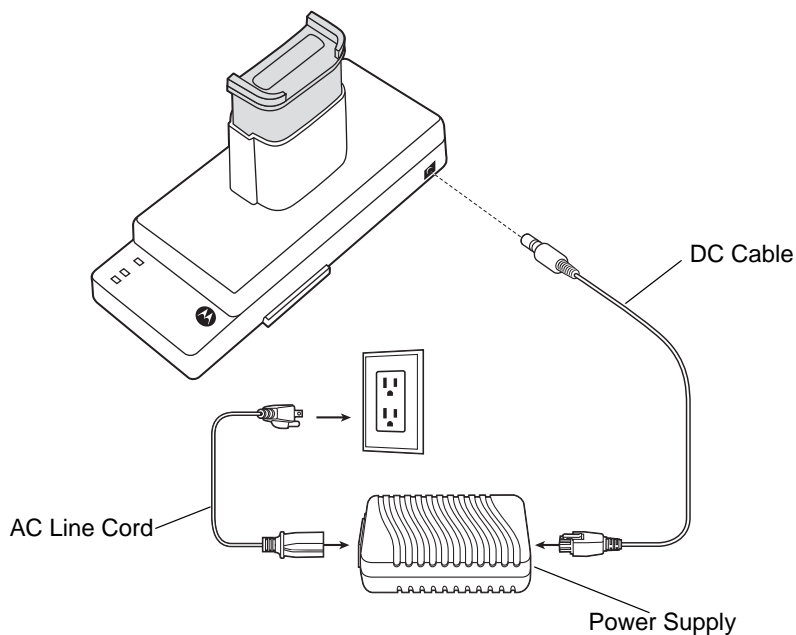
**Figure 2-28**   *UBC Adapter Power Connection*

Battery Charging Indicators

To charge a spare battery using the UBC adapter, connect the power supply to the UBC (see *Figure 2-28 on page 2-27*), then insert the spare battery. The spare battery begins charging automatically. The UBC's charge LEDs (see *Figure 2-29*)) show the status of the battery charging in the adapter. *Table 2-7* shows battery charging status indications. The battery usually charges in three hours.
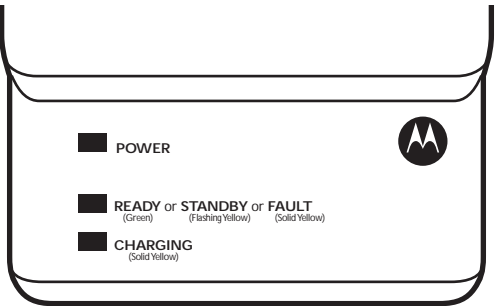
Figure 2-29   *UBC Adapter LEDs*

Table 2-7   *UBC Adapter Charge LED Status Indications*

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

Table 2-7   *UBC Adapter Charge LED Status Indications (Continued)*

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.

Modem Module

This section describes how to setup and use the MDM9000 Modem Module.
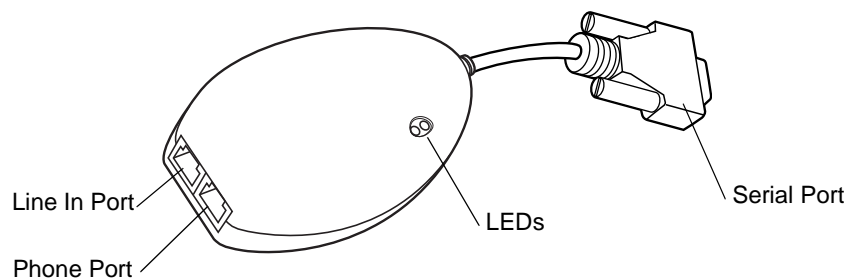
Figure 2-30   *Modem Module*

The Modem Module enables data communication between the mobile computer and a host computer, remotely through the phone lines, and synchronizes information between the mobile computer and a host computer.

The following items are required for a modem connection:

- Telephone number, IP address and DNS/WINS address information from the dial-in server administrator
- Dial-in account on the host system, including a user ID and password
- RJ11 or RJ12 modem cable
- Functioning telephone jack that supports plug-in modems connected to the local telephone system
  Setup of Country Codes to use the modem with the appropriate country's telephone network.

The following items are required for communication:

- MC909X mobile computer
- Cable Adapter Module (CAM), Symbol p/n ADP9000-100 (see *Cable Adapter Module on page 2-23*)
- Serial Adapter Cable (for communication via cradle), Symbol p/n 25-63856-01
- Microsoft ActiveSync
  Setup of host computer and mobile computer.

Setup

Connecting to the Mobile Computer
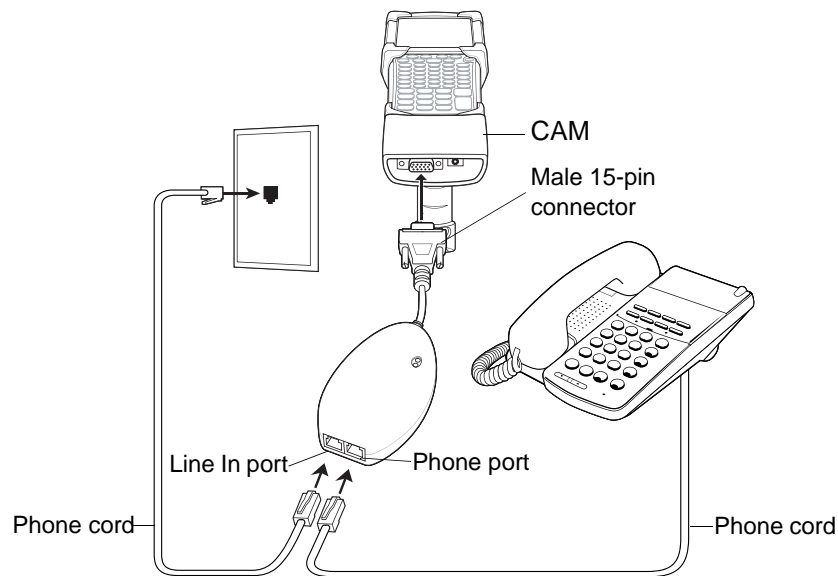
Figure 2-31 *Modem Module Connection - Mobile Computer*

> ⚠ **CAUTION** Do not connect the modem's 15-pin connector into a VGA port of a host computer.

Using the Correct Telephone Line Type

Use a standard analog phone line, as in most households. In an office, use a line connected to a fax machine or modem. In a hotel, request a room with a standard phone line or data port. If necessary, check with the local phone company or administrator to make sure you are using the right type of line before sending data.

Connecting to the Single Slot Serial/USB Cradle

Adapter cable

Male 15-pin connector

Line In port

Phone cord
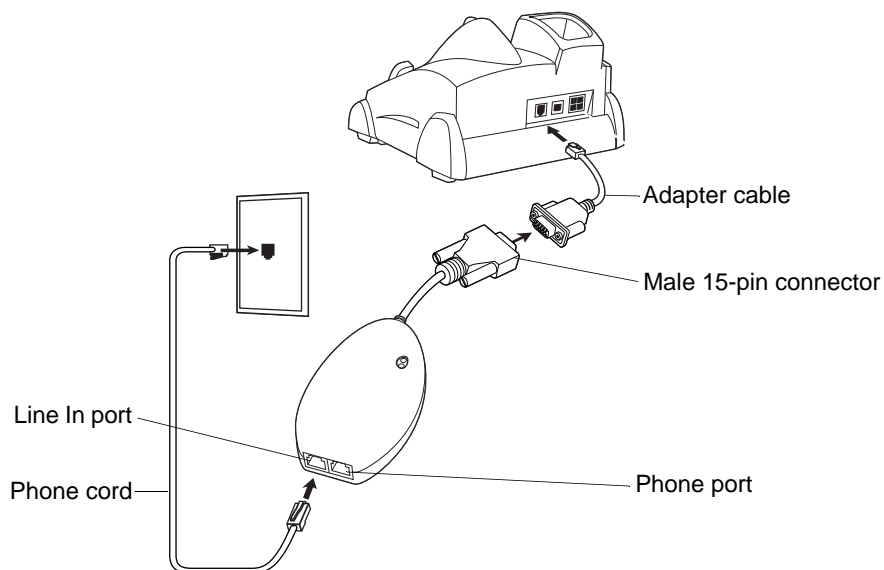
Phone port

Figure 2-32   *Modem Module Connection - Single Slot Serial/USB Cradle*

⚠️ *CAUTION*   Do not connect the modem's 15-pin connector into a VGA port of a host computer.

✓ *NOTE*   If using a phone, connect the cord from the phone to the Phone port on the modem.

Table 2-8   *Modem Indicators*

LED	Indication
Off	Modem is not properly connected to the mobile computer; modem is not receiving power.
Green	Modem is connected to the mobile computer and is receiving power.
Solid Amber	Mobile computer is communicating with the host computer.

Configuring the Mobile Computer for the Modem (Windows Mobile 5.0)

✓ *NOTE*   To edit an existing modem connection using *Manage existing connections*, see *Changing the Initialization String (Windows Mobile 2005) on page 2-36*.

To create a new modem connection on the mobile computer:

1. Connect the modem to the mobile computer as described in *Connecting to the Mobile Computer on page 2-29*.

2. Tap **Start** > **Settings** > **Connections** tab > **Connections** icon.

3. In the **Connections** window, select **Add a new modem connection** to create a connection.
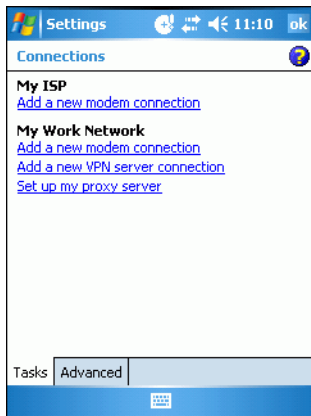
Figure 2-33 *Connections Window*

4. Enter a name for the connection. In the drop-down menu, select **Hayes Compatible on COM1**, then tap **Next**.
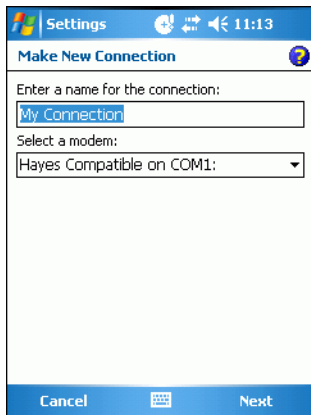
Figure 2-34 *New Connection Window*

5. Enter the access phone number in the **My Connection** window and tap **Next**.
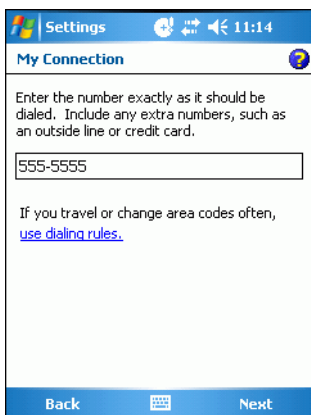
Figure 2-35 *My Connection Window - Phone Number*

NOTE   Depending on the location when dialing, additional numbers may need to be dialed (e.g., a 9 prefix is often required if dialing from work; a country code is needed if dialing internationally). To avoid creating new modem connections for each situation, tap **use dialing rules** to define frequently used dialing locations.

6. If necessary, enter the user name, password and domain.
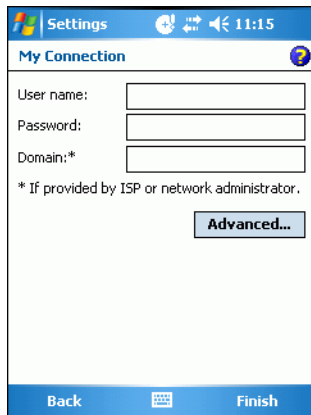
Figure 2-36 *My Connection Window - User Information Settings*

7. Tap **Advanced...** to edit the **Extra dial-string modem commands:** text box to set country parameters to operate the modem with other country telephone networks.
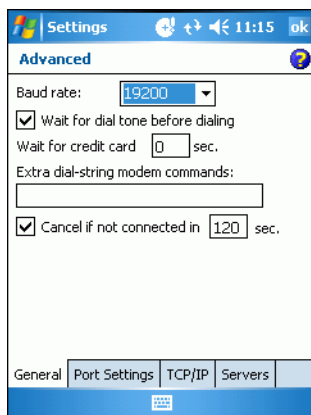
Figure 2-37 *Advanced Window - Extra Dial-String Modem Commands*

The modem defaults to operation with US telephone networks (country code: B5). To operate the modem with other country telephone networks, a country code must be entered. The modem adjusts its operating parameters to comply with the telephone network in the country specified. See *Modem Country Setup on page 2-35* for the appropriate syntax and a list of country codes.

8. Tap **ok** to exit the **Advanced** window.

9. Tap **Finish**.

Configuring the Mobile Computer for the Modem (Windows CE 5.0)

To create a modem connection on the mobile computer:

1. Connect the modem to the mobile computer, see *Connecting to the Mobile Computer on page 2-29*.

2. On the MC909X, tap **Settings** > **Control Panel**. Double-tap the **Network and Dial-up Connections** icon.

3. In the **Connection** window, double-tap **Make New Connection** to create a connection.
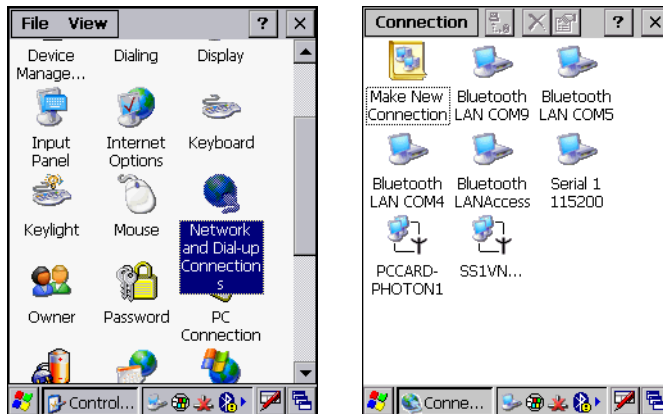
Figure 2-38   *Network and Connections Windows*

4.   Enter a name for the connection on the **Make New Connection** window, then tap **Next**.

5.   In the **Select a modem** list, select **Hayes Compatible on COM1**, then tap **Next**.
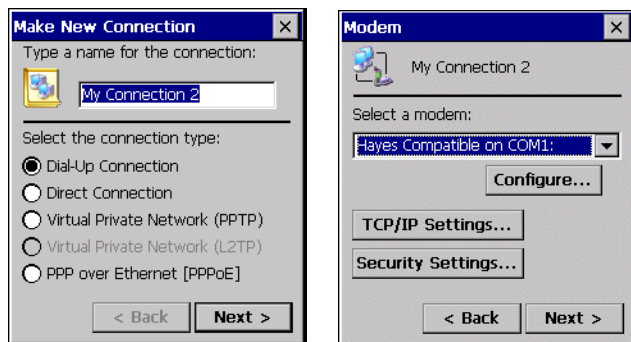
Figure 2-39   *New Connection and Modem Windows*

6.   In the **Phone Number** window, enter the phone number for the connection, then tap **Finish**.
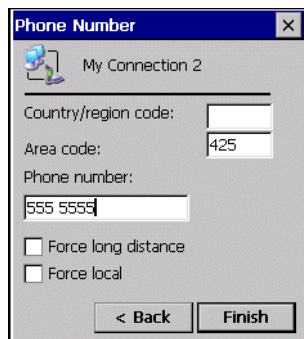
Figure 2-40   *Phone Number Window*

NOTE   Depending on the location when dialing, additional numbers may need to be dialed (e.g., a 9 prefix is often required if dialing from work; a country code is needed if dialing internationally). To avoid creating new modem connections for each situation, tap *use dialing rules* to define frequently used dialing locations.

Connecting the Modem (Windows Mobile 5.0)

To start the connection:

1. Tap **Start** > **Settings** > **Connections** tab > **Connections**.

2. In the **Connections** window, tap **Manage existing connections**.
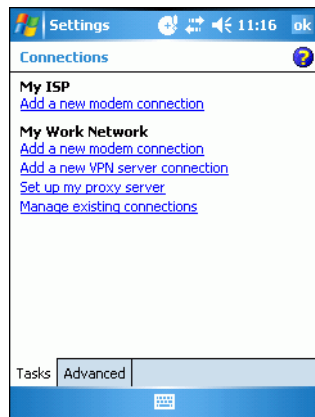
Figure 2-41   *My Connections Window*

3. Tap and hold the connection name, then select **Connect** from the menu that appears. The modem attempts to connect.
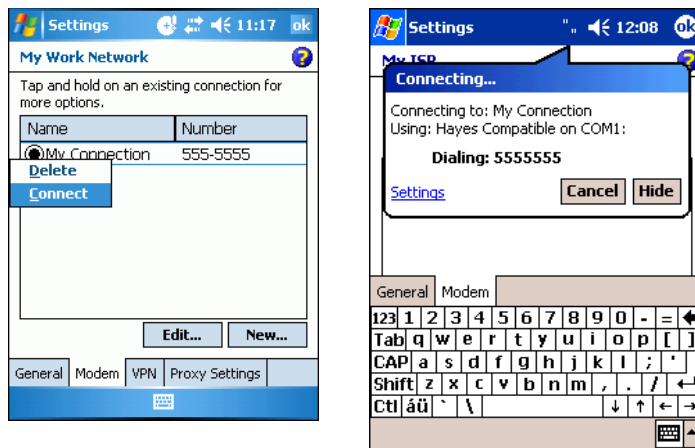
Figure 2-42   *Creating a Connection*

Connecting the Modem (Windows CE 5.0)

To connect to the host computer using the modem connection created in the last section:

1. Tap **Start** > **Settings** > **Control Panel**. Double-tap the **Network and Dialup Connections** icon.

2. In the **Connection** window, double-tap the name of the connection created in Creating a *Connecting the Modem (Windows CE 5.0) on page 2-34*.

3. To modify dial-up properties, tap **Dial Properties...**, make the selections in the **Device Properties** window, then tap **OK**.

4. Tap **Connect**. The modem attempts to connect.
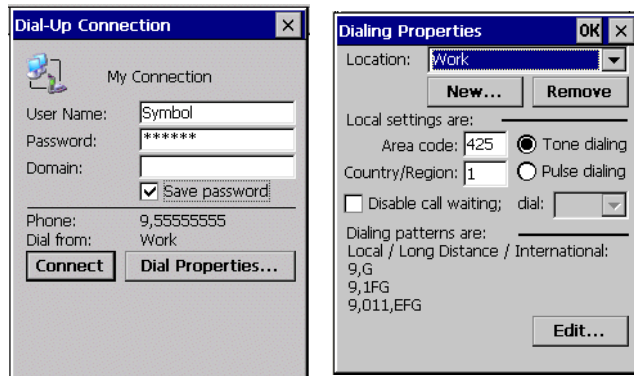
Figure 2-43   *Dial-Up and Dial Properties Window*

Modem Country Setup

Edit the *Extra dial-string modem commands:* text box in the mobile computer to set country parameters. The syntax used is: +GCI=<country_code>.

Supported Countries

Table 2-9   *Supported Countries*

Country	Code	Country	Code	Country	Code
Australia	09	Greece	FD or 46	Norway	FD or 82
Austria	FD or 0A	Iceland	FD	Portugal	FD or 8B
Belgium	FD or 0F	Ireland	FD or 57	Spain	FD or A0
Brazil	16	Italy	FD or 59	Sweden	FD or A5
Canada	20	Liechtenstein	FD	Switzerland	FD or A6
Denmark	FD or 31	Luxembourg	FD	TBR-21 (Europe)	FD
Finland	FD or 3C	Mexico	73	United Kingdom	FD or B4
France	FD or 3D	Netherlands	FD or 7B	United States	B5 (Default)
Germany	FD or 42	New Zealand	7E		

Note: Use FD where possible. If connection problems occur, use the alternate code where provided.

AT Commands

The AT Command Set allows you to custom-configure the modem.

> *NOTE*   Only experienced users having difficulty with default settings should use this feature.

Changing the Initialization String (Windows Mobile 2005)

To enter AT commands:

1. Tap **Start** > **Settings** > **Connections** tab > **Connections** icon.

2. If creating a new connection, select **Add a new modem connection** in the **Connections** window. Then follow steps 1 through 6 in *Configuring the Mobile Computer for the Modem (Windows Mobile 5.0) on page 2-30* and proceed to step 6.
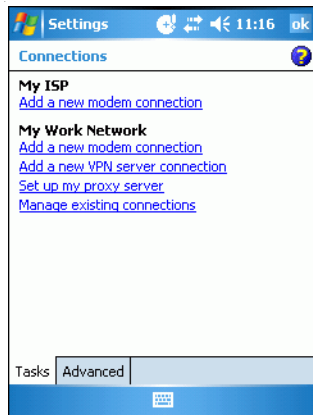
Figure 2-44   *Connections Window*

3. If entering AT commands for an existing connection, select **Manage existing connections** in the **Connections** window.

4. On the **Modem** tab, select the radio button of the item to edit and tap **Edit...** .
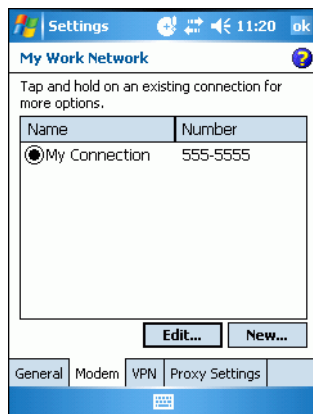
Figure 2-45   *New Connection Window*

5. Tap **Next** until the **User Information Settings** window appears.

6. Tap **Advanced...** .
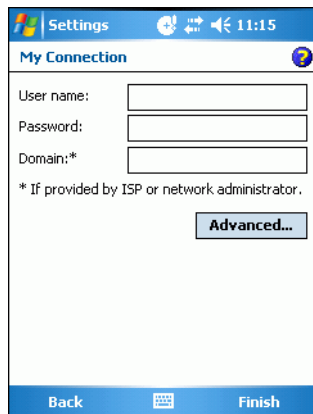
Figure 2-46   *My Connection Window - User Information Settings*

7.   Enter AT commands in the **Extra dial-string modem commands:** text box. See *Basic AT Command Syntax on page 2-39*.
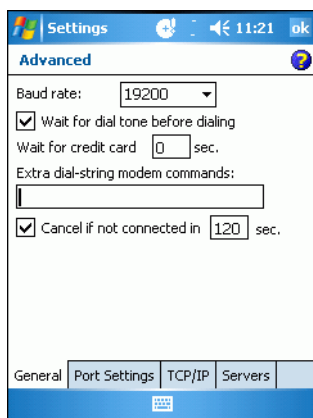
Figure 2-47   *Advanced Window - Extra Dial-String Modem Commands*

8.   Tap **ok** to exit the *Advanced* window.

9.   Tap **Finish**.

Changing the Initialization String (Windows CE 5.0)

To enter AT commands:

1.   On the mobile computer, tap **Settings** >**Control Panel**. Double-tap the **Network and Dial-up Connections** icon.

2.   In the **Connection** window, double-tap the **My Connection** icon to edit the settings.
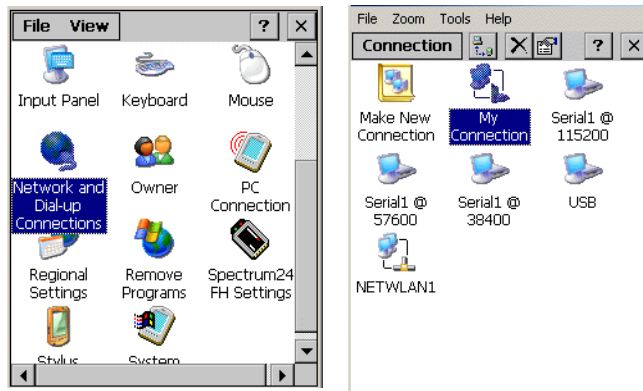
Figure 2-48   *Network and Connections Windows*

3.   To modify dial-up properties, tap **Dial Properties**, make the selections in the **Device Properties** window.

4.   To edit the **Dialing Patterns**, tap **Edit**.
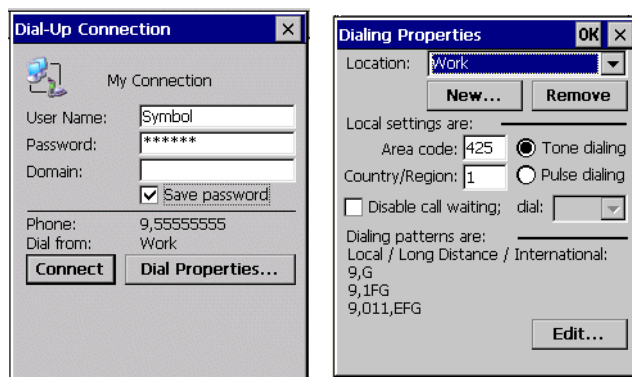
Figure 2-49   *Dial-Up and Dial Properties Window*

5.   The **Edit Dialing Patterns** window appears.
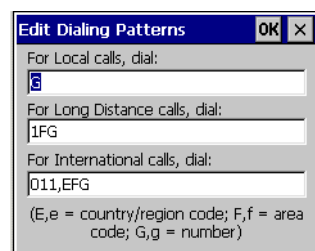
Figure 2-50   *Edit Dialing Patterns Window*

6.   Edit the dialing properties, see *Table 2-10 on page 2-40*.

7.   Tap **OK** to exit the **Edit Dialing Patterns** window.

8.   Tap **OK** to exit the **Dialing Patterns** window.

9.   Tap **Connect** at the Dial-Up Connection window. The modem attempts to connect.

Basic AT Command Syntax

A command line is made up of three elements:

- **Prefix** - consists of the characters "AT" or "at" or, to repeat the execution of the previous command line, "A/" or "a/".

- **Body** - made up of individual commands described later. Space characters (IA5 2/0) are ignored and may be used for formatting purposes, unless they are embedded in numeric or string constants. The termination character may not appear in the body. The modem can accept at least 40 characters in the body.

- **Termination character** - may be selected by a user option (parameter S3). The default is CR.

The format of Basic Syntax commands, except for the D and S commands, is as follows:

<command>[<number>]

where:

- <command> is either a single character, or the "&" character followed by a single character per V.250; or the "%" character followed by a single character, the "*" character followed by a single character, or the "^" character followed by a single character.

- <number> is a string of one or more characters from "0" through "9" representing a decimal integer value. Commands expecting a <number> are noted in the description of the command. If <number> is missing from such a command (<command> is immediately followed by another <command> or the termination character), the value "0" is assumed. If a command does not expect a <number> and a number is present, an error occurs. All leading "0"s in <number> are ignored by the modem.

Additional commands may follow a command (and associated parameter, if any) on the same command line with a separation character. The actions of some commands cause the rest of the command line to be ignored.

S-Parameters

Commands that begin with the letter "S" are known as "S-parameters". The number following the "S" indicates the "parameter number" referenced. If the number is not recognized as a valid parameter number, an ERROR result code issues. Immediately following this number, either a "?" or "=" character must appear. "?" is used to read the current value of the indicated S-parameter; "=" sets the S-parameter to a new value.

S<parameter_number>?

S<parameter_number>=[<value>]

If the "=" is used, the new value to be stored in the S-parameter is specified in decimal following the "=". If no value is given (i.e., the end of the command line occurs or the next command follows immediately), the S-parameter specified may be set to 0, or an ERROR result code issues and the stored value remains. The ranges of acceptable values are given in the description of each S-parameter.

If the "?" is used, the modem transmits a single line of information text to the DTE. The text portion of this information text consists of exactly three characters, giving the value of the S-parameter in decimal, with leading zeroes included.

Commands

The tables that follow summarize the AT commands, result codes, and S-Registers for the MDM 3000. **<string>** represents a letter, number, or symbol to be entered. **<value>** represents a number to be entered. Possible values are listed below the command.

Table 2-10   *AT Command Table*

Command	Description		Country Specific
D	Dial "D<string>"		
	0-9	DTMF digits 0-9	
	*	The 'star' digit (tone dialing only)	
	#	The 'gate' digit (tone dialing only)	
	A-D	DTMF digits A,B,C,D	X
	L	Re-dial last number	
	P	Pulse dialing	X
	T	Tone dialing	
	W	Wait for dial tone. (Modem waits for dial tone before dialing digits following "W".)	
	@	Wait for silence. (Modem waits for at least 5 seconds of silence in the call progress frequency band before continuing with next dial string parameter.)	
	&	Wait for credit card dialing tone before continuing with the dial string.	
	'	Dial pause. (Modem pauses for a time specified by S8 before dialing the digits following ",")	
	;	Return to command state. (Modem goes off hook and allows entering additional AT commands. Use "H" to go back to on hook.)	
	() - <space>	Ignored. (Might be used to format the dial string.)	
A	Off-hook and attempt to answer a call		
H	Disconnect – Hang UP		
O	Return to On-Line Data Mode. O <value>		
	0	Enters on-line data mode without a retrain.	
	1	Enters on-line data mode with a retrain.	
L	Speaker volume (Not used)		
M	Speaker control. M <value>		
	0	Always off.	
	1	On during call establishment. Off when receiving carrier. (default)	

Table 2-10   *AT Command Table (Continued)*

Command	Description		Country Specific
	2	Always on.	
	3	Off when receiving carrier and during dialing. On during answering.	
&G	Guard tone. &G<value>		X
	0	Disables guard tone. (default)	
	1	Disables guard tone.	
	2	Select 1800 Hz guard tone.	
&V1	Displays last connection statistics		
+MS	Modulation Selection. +MS=<carrier>		X
	B103	Bell 103 (300)	
	B212	Bell 212 (1200 Rx/75 or 75Rx/1200 Tx)	
	V21	300	
	V22	1200	
	V22B	2400 or 1200	
	V23C	1200	
	V32	9600 or 4800	
	V32B	14400, 12000, 9600, 7200 or 4800	
	V34	33600, 31200, 28800, 26400, 2400, 21600, 19200, 16800, 14400, 12000, 9600, 7200, 4800 or 2400	
%E	Enable/Disable Line Quality Monitor and Auto-Retrain or Fall back/Fall forward. %E<value>		
	0	Disable line quality monitor and auto re-train.	
	1	Enable line quality monitor and auto re-train.	
	2	Enable line quality monitor and fallback/fall forward. (default).	
B	CCITT or Bell. B<value>		
	0	Select CCITT operation at 300 or 1200 bauds.	
	1	Selects Bell operation at 300 or 1200 bauds.	
&L	Leased Line Operation. &L<value>		
	0	Requests dial-up operation. Dial-up operation continues.	

Table 2-11   *S-Register Settings*

Reg	Function	Range	Default Default	Default Saved	Units
S0	Rings to Auto Answer	0-255	0	*	rings
S1	Ring Counter	0-255	0	*	rings
S2	Escape Character	0-255	43		ASCII
S3	Carriage Return Character	0-127	13		ASCII
S4	Line Feed Character	0-127	10		ASCII
S5	Backspace Character	0-255	8		ASCII
S6	Wait Time before Blind Dialing or Dial Tone	2-255	2	*	S
S7	Wait Time for Carrier, Silence or Dial Tone	1-255	50	*	S
S8	Pause Time for Dial Delay Modifier	0-255	2	*	S
S9	Carrier Detect Response Time	1-255	6	*	0.1 S
S10	Lost Carrier to Hangup Delay	1-255	14	*	0.1 S
S11	DTMF Tone Duration	50-255	95	*	mS
S12	Escape Prompt Delay (EPD)	0-255	50	*	.02 S
S14	General Bit Mapped Options Status	-	138 (8Ah)		
S16	Test Mode Bit Mapped Options Status	-	0		
S19	Reserved	-	0		
S20	Reserved	-	0		
S21	V.24 Bit Mapped Options Status	-	52 (34h)		
S22	Speaker/Results Bit Mapped Options	-	117 (75h)		
S23	General Bit Mapped Options Status	-	62 (3Dh)		
S24	Sleep Inactivity Timer	0-255	0		S
S25	Delay to DTR off	0-255	5		S
S26	RTS-to-CTS Delay	0-255	1		.01 S
S27	General Bit Mapped Options Status	-	73 (49h)		
S28	General Bit Mapped Options Status	-	0		
S29	Flash Dial Modifier Time	0-255	70		10 mS
S30	Disconnect Inactivity Timer	0-255	0		10 S

* Register value may be stored in on of two user
** Country-dependent

Table 2-11   *S-Register Settings (Continued)*

Reg	Function	Range	Default — Default	Default — Saved	Units
S31	General Bit Mapped Options Status	-	195 (C0h)		
S36	LAPM Failure Control	-	7	*	
S38	Delay Before Forced Hangup	0-255	20		S
S39	Flow Control Bit Mapped Options Status	-	3		
S40	General Bit Mapped Options Status	-	104 (68h)	*	
S41	General Bit Mapped Options Status	-	195 (C3h)	*	
S46	Data Compression Control	-	138	*	
S48	V.42 Negotiation Control	-	7		
S86	Call Failure Indication	0-26	0		
S91	PSTN Transmit Attenuation Level	0-15	10**		dBm
S92	Fax Transmit Attenuation Level	0-15	10**		dBm
S95	Extended Result Codes Control		0	*	
S210	V.34 Symbol Rate	0-255	13 (0Dh)		

* Register value may be stored in on of two user
** Country-dependent

Serial Communication Setup

The serial communications setup can be used to set up to communicate with a Single Slot Serial/USB Cradle, MSR or a CAM.

> **NOTE**   For serial communication using accessories that can communicate with either a serial or USB connection, connect only the serial cable. Do not connect both the serial and USB cables. If both serial and USB communication cables are required, the host computer's USB port must be disabled in ActiveSync before serial communication can be enabled.

Setting Up a Connection on the Mobile Computer (Windows Mobile 2005)

1. On the mobile computer tap **Start** > **Programs** > **ActiveSync** to display the **ActiveSync** window.
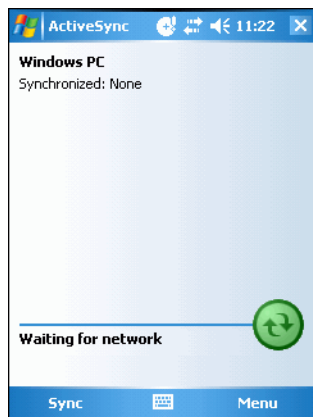
Figure 2-51   *ActiveSync Window*

2. Tap **Menu** > **Connections**. The **Connections** window appears.
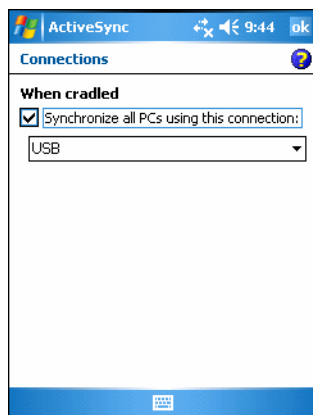
Figure 2-52   *Connections Window*

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.
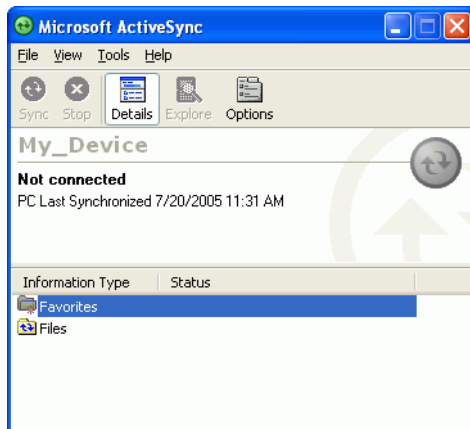
Figure 2-53   *ActiveSync - Not Connected*

> **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.

Figure 2-54   *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.

Serial Connection Setup (Windows CE 5.0)

1. On the mobile computer tap **Start** > **Settings** > **Control Panel** > **PC Connection** icon.
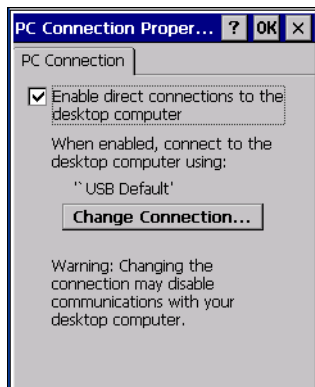
Figure 2-55   *PC Connection Properties Window*

2. Tap **Change Connection...** .
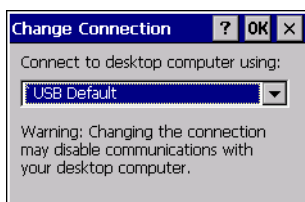
Figure 2-56   *Change Connection Window*

3. Select the serial communication type from the drop-down list.

4. Tap **OK**.

5. Tap **OK**.

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

7. Start ActiveSync if it is not running on the host computer. To start, select **Start** > **Programs** > **Microsoft ActiveSync**.
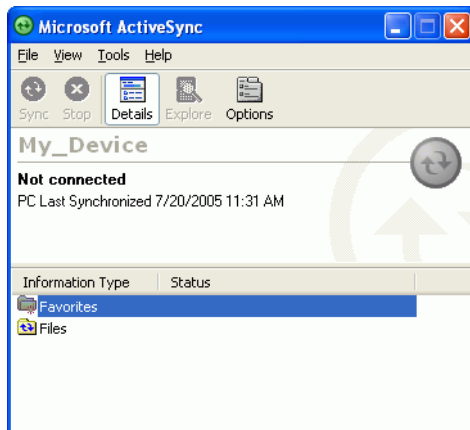
Figure 2-57   *ActiveSync - Not Connected*

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

Figure 2-58   *Connection Settings*

9. For a serial connection, select **Allow connections to one of the following:** check box and select the comm port from the drop-down list.

10. For USB connection, select **Allow USB connection** check box.

11. 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.

12. Connect the device to the host computer.

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

13. Upon connection, synchronization occurs automatically.

USB Host Communication Setup

> **NOTE**   USB Host mode is only available on Windows Mobile 5.0 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.
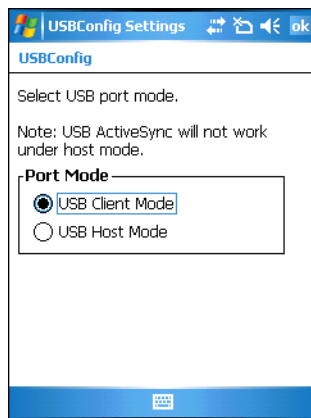
Figure 2-59   *USBConfig Settings Window*

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.

Wall Mounting Bracket and Shelf Slide

This section describes how to install and set up the MC9000 Wall Mount Bracket and Shelf Slide to mount cradles to a wall.

Wall Mounting Bracket

Shelf Slides

Mounts one single slot cradle   Mounts two single slot cradles
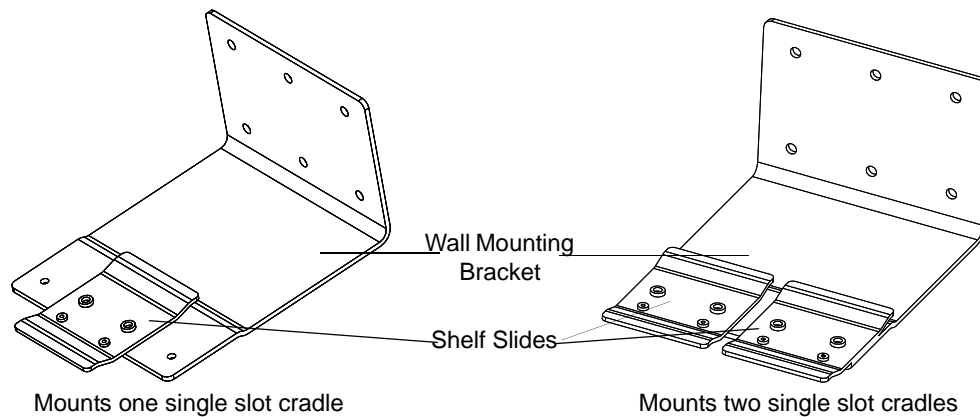
Figure 2-60   *Wall Mounting Bracket with Shelf Slide*

When installed on a wall, the mounting bracket and shelf slide enable mounting one or two single slot cradles to a wall. Use two brackets to mount a four slot cradle.
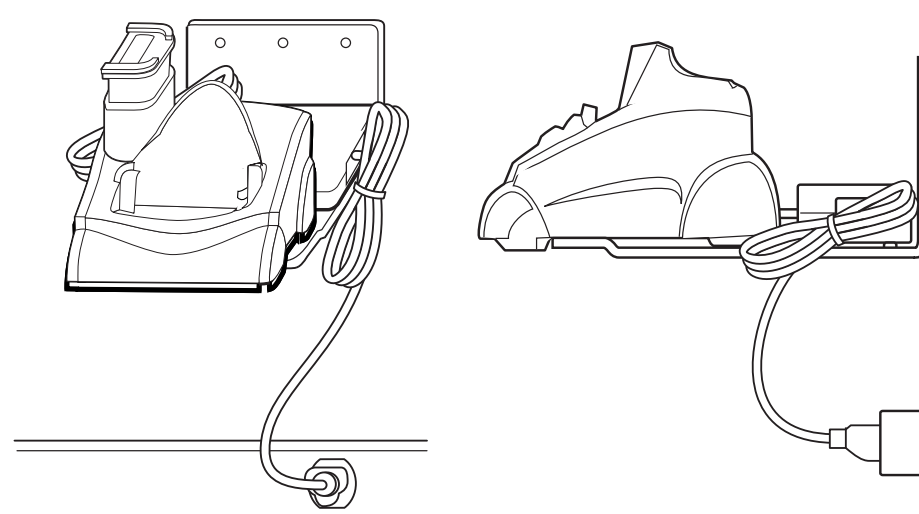
Figure 2-61   *Mounted Single Slot Cradle With Power Connection*

Installing the Wall Mount Bracket

To install the wall mount bracket for use with one or two single slot cradles or four slot chargers, place the smaller surface of the bracket against the wall or vertical support structure, and secure with four 1/4" screws (use two of the three screw holes in each row).
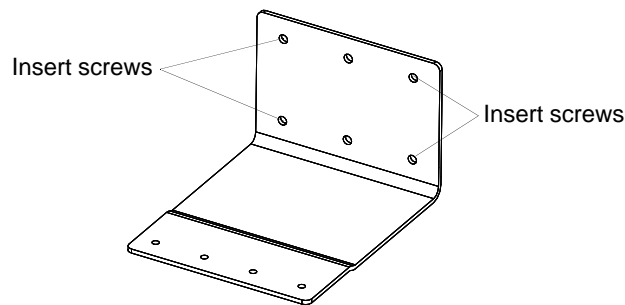
Figure 2-62 *Wall Mounting Bracket Mounting Screws*

If using the bracket and slide with a four slot cradle, secure a second bracket to the wall next to the first, aligning the horizontal screw holes on the second with those of the first.

Attaching the Shelf Slide to the Wall Mount Bracket

One Single Slot Cradle/Four Slot Battery Charger

To attach the shelf slide to the wall mount bracket for use with one single slot cradle or four slot battery charger:

1. Place the slide on the bracket, aligning the larger pan-head screw holes in the slide with the center two screw holes on the bracket.

2. Secure the slide to the bracket by inserting the two pan-head screws provided from below the bracket, up through the bracket's screw holes and then through the slide's pan-head screw holes.
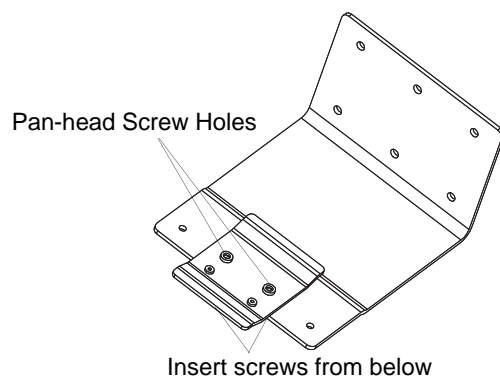
Figure 2-63 *Attaching One Shelf Slide*

Two Single Slot Cradles/Four Slot Battery Chargers

To attach the shelf slide to the wall mount bracket for use with two single slot cradles or two four slot battery chargers:

1. Place the slide on the bracket, aligning the larger pan-head screw holes in the slide with the left or right two screw holes on the bracket.

2. Secure the slide to the bracket by inserting the two pan-head screws provided from below the bracket, up through the bracket's screw holes and then through the slide's pan-head screw holes.

3. Secure a second slide to the remaining two screw holes on the bracket in the same manner.
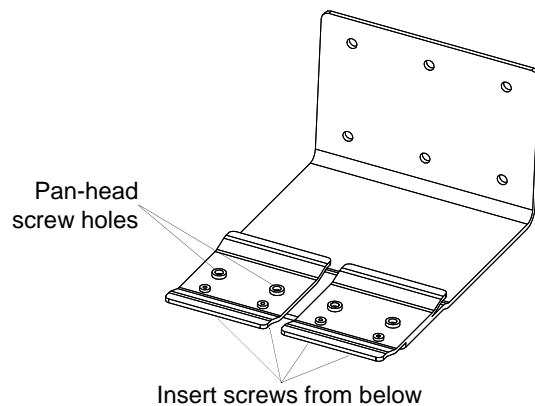
Figure 2-64   *Attaching Two Shelf Slides*

Four Slot Cradle

To attach the shelf slide to the wall mount bracket for use with a four slot cradle:

1. Place a slide on the left-hand bracket, aligning the larger pan-head screw holes in the slide with the left two screw holes on the bracket.

2. Secure the slide to the bracket by inserting the two pan-head screws provided from below the bracket, up through the bracket's screw holes and then through the slide's pan-head screw holes.

3. Place a slide on the right-hand bracket, aligning the larger pan-head screw holes in the slide with the right two screw holes on the bracket.

4. Secure the second slide to the bracket as described in Step 2.

Installing the Cradle/Charger on the Bracket

Install the cradle or charger onto the bracket, inserting the bracket's slide into the grooves on the bottom of the cradle/charger and sliding the cradle/charger into the desired position.

For one single slot cradle/four slot charger, center it on the bracket.

Slide grooves on bottom of
cradle/charger over bracket slide
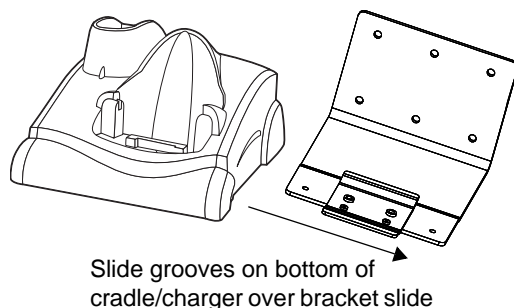
Figure 2-65   *Attaching Two Shelf Slides*

For two single slot cradle/four slot chargers, slide one onto the left-hand slide, and one onto the right-hand slide.

Insert set screws
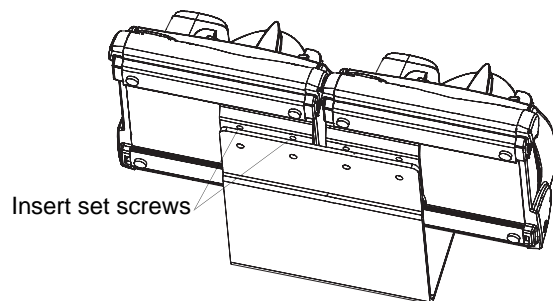
Figure 2-66   *Attaching Two Shelf Slides*

For a four slot cradle, slide the cradle on to the slides, across both brackets.

Secure each cradle or charger to its slide using the two set screws provided.

Chapter 3 ActiveSync

Introduction

To communicate with various host devices, install Microsoft ActiveSync (version 4.1 or higher) on the host computer. Use ActiveSync to synchronize information on the 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 5.0 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 4.1 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.
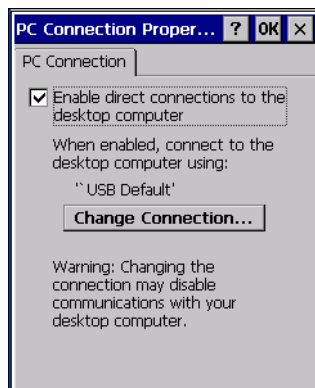
Figure 3-1   *PC Connection Properties Window*

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 5.0 Devices:

1. On the mobile computer tap **Start** > **Programs** > **ActiveSync** icon. The **ActiveSync** window appears.
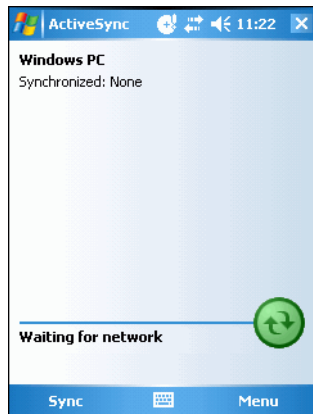
Figure 3-2   *ActiveSync Window*

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.
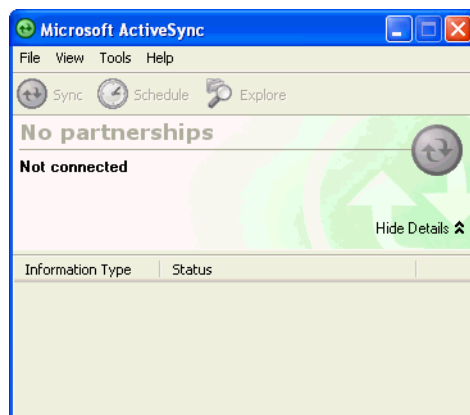
Figure 3-3   *ActiveSync Window*

> **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.

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**.
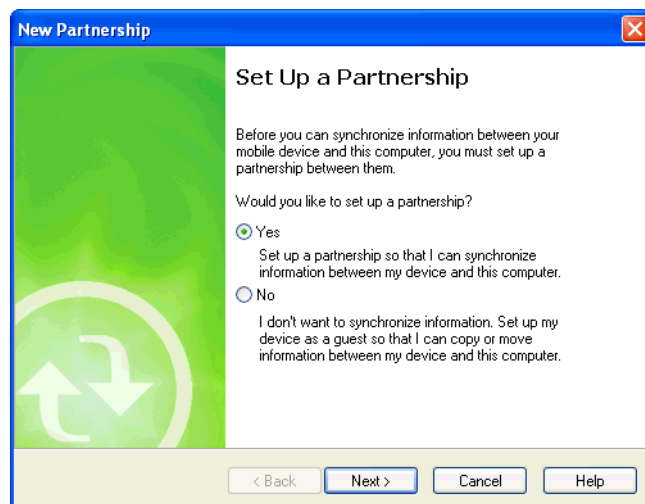
Figure 3-5   *New Partnership Window*

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

3.   Click **Next**.
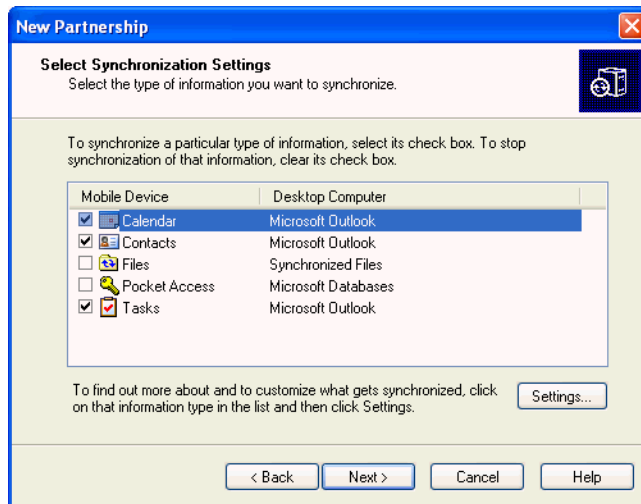
Figure 3-6   *Select Synchronization Setting Window*

4.   Select the appropriate settings and click **Next**.
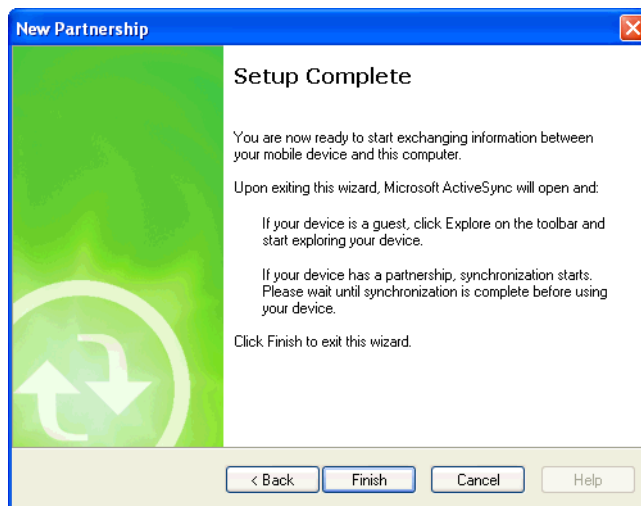
Figure 3-7   *Setup Complete Window*

5.   Click **Finish**.
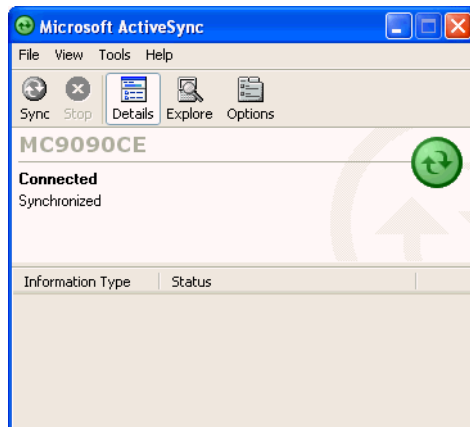
Figure 3-8   *ActiveSync Connected Window*

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 SMDK Windows CE Help File for Symbol Mobile Computers.

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

Synchronization with a Windows Mobile 5.0 Device

> *NOTE*   When a mobile computer with Windows Mobile 5.0 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 5.0 device:

1.   If the **Get Connected** window does not appear on the host computer, select **Start** > **All Programs** > **Microsoft ActiveSync**.
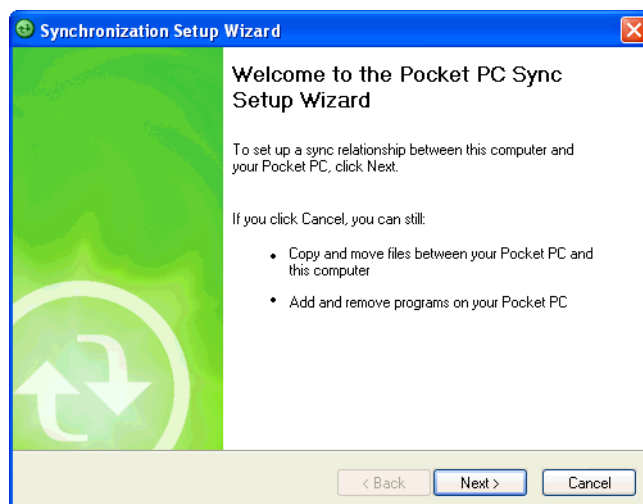
Figure 3-9   *Synchronization Setup Wizard Window*

2. Click **Next**.
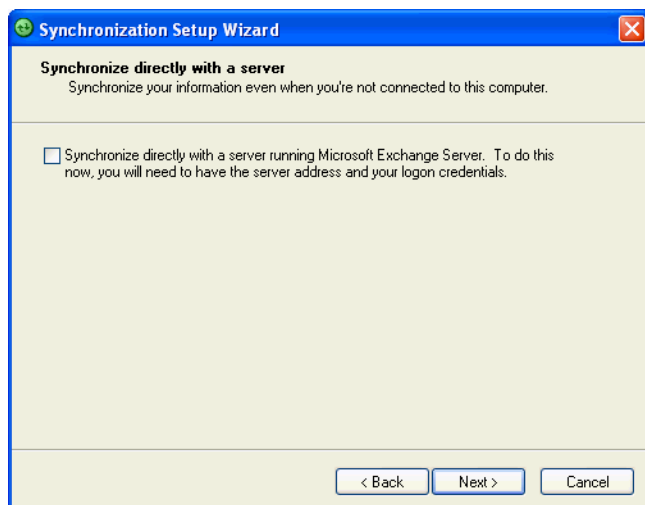
Figure 3-10   *Synchronization Directly With a Server Window*

3. Select the check box to synchronize with a server running Microsoft Exchange.

4. Click **Next**.
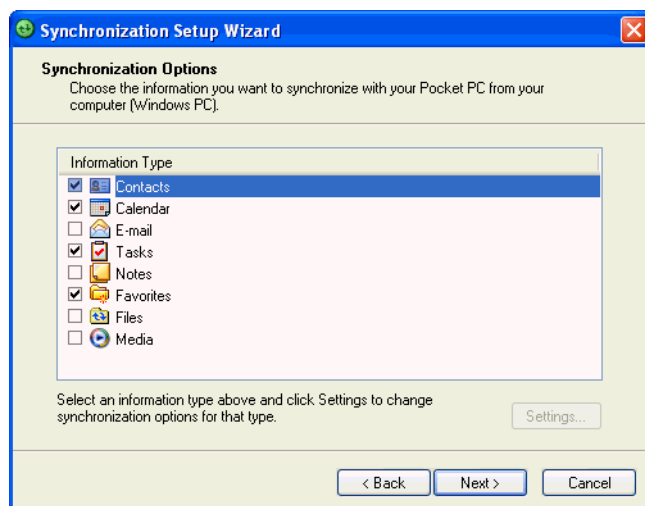
Figure 3-11   *Synchronization Option Window*

5. Select the appropriate settings and click **Next**.
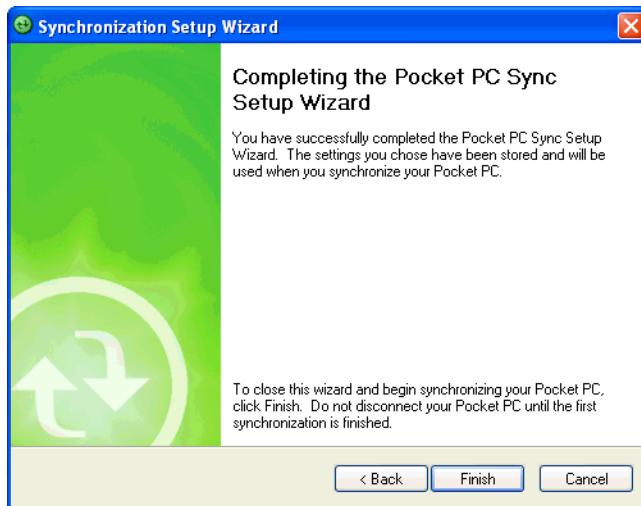
Figure 3-12   *Wizard Complete Window*

6.   Click **Finish**.
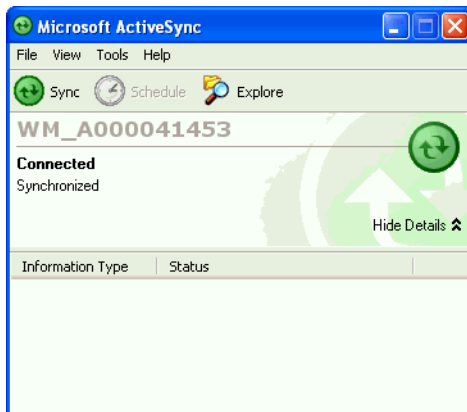
Figure 3-13   *ActiveSync Connected Window*

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 Wireless Applications

Introduction

Wireless Local Area Networks (WLANs) allow mobile computers to communicate wirelessly and send captured data to a host device in real time. The MC909X mobile computer supports the IEEE 802.11a, 802.11b and 802.11g standards. Before using the mobile computer on a WLAN, the facility must be set up with the required hardware to run the wireless LAN and the mobile computer must be configured. Refer to the documentation provided with the access points (APs) for instructions on setting up the hardware.

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

- Wireless Status
- Wireless Diagnostics
- Find WLANs
- Manage Profiles
- Options
- Enable/Disable Radio (not available on Windows CE 5.0 devices with Fusion 2.3 and lower)
- Log On/Off.

Tap the **Signal Strength** icon to display the **Wireless Applications** menu.
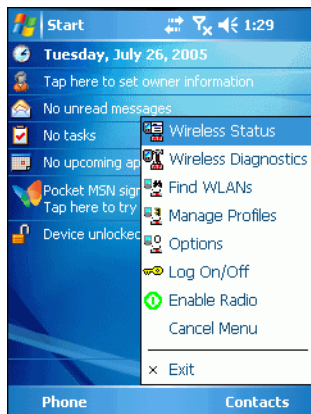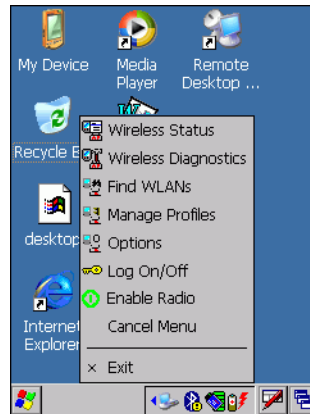
Windows Mobile 5.0   Windows CE 5.0

Figure 4-1   *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 4-1   *Wireless Applications Icons, Signal Strength Descriptions*

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

Turning the WLAN Radio On and Off

Windows Mobile 5.0

To turn the WLAN radio off tap the **Signal Strength** icon and select **Disable Radio**.

Figure 4-2   *Disable Radio*

To turn the WLAN radio on tap the **Signal Strength** icon and select **Enable Radio**.
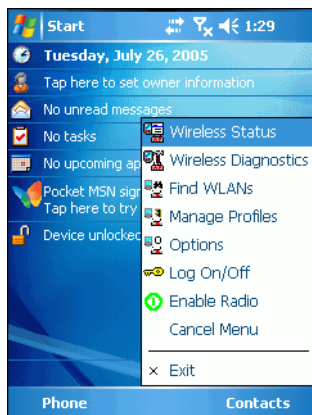
Figure 4-3   *Enable Radio*

NOTE For Windows Mobile 5.0 devices with AKU 2.2 and higher, the WLAN radio can also be turned on and off using the Wireless Manger. See *Turning Off the Radios on page 1-21*.

Windows CE 5.0 with Fusion 2.3 and Lower

To turn the WLAN radio off:

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 the WLAN radio on:

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**.

Windows CE 5.0 with Fusion 2.4 and Higher

To turn the WLAN radio off tap the **Signal Strength** icon and select **Disable Radio**.

Figure 4-4   *Disable Radio*

To turn the WLAN radio on tap the **Signal Strength** icon and select **Enable Radio**.
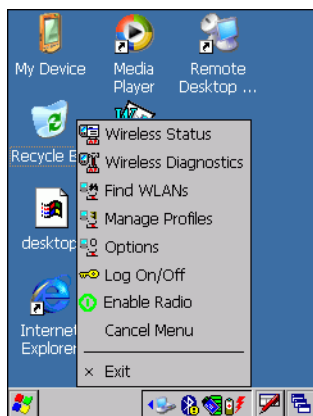
Figure 4-5   *Enable Radio*

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.
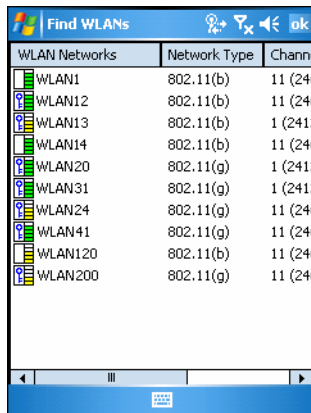
Figure 4-6   *Find WLANs Window*

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

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

The *Find WLANs* list displays:

- WLAN Networks - Available wireless networks with icons that indicate signal strength and encryption type. The signal strength and encryption icons are described in *Table 4-2* and *Table 4-3*.
- Network Type - Type of network.
- Channel - Channel on which the AP is transmitting.
- Signal Strength - The signal strength of the signal from the AP.

Table 4-2   *Signal Strength Icon*

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

Table 4-3 *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 open a pop-up menu which provides two options: **Connect** and **Refresh**. Select **Refresh** to refresh the WLAN list. Select **Connect** to create a wireless profile from that network. This starts the **Profile Editor Wizard** which allows you to set the values for the selected network. After editing the profile, the mobile computer automatically connects to this new profile.

Profile Editor Wizard

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

Navigate through the wizard using the **Next** and **Back** buttons. Tap **X** to quit. On the confirmation dialog box, tap **No** to return to the wizard or tap **Yes** to quit and return to the *Manage Profiles* window. See *Manage Profiles Application on page 4-22* for instructions on navigating the **Profile Editor Wizard**.

Profile ID

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

Figure 4-7 *Profile ID Dialog Box*

Table 4-4 *Profile ID Fields*

Field	Description
Name	The name and (WLAN) identifier of the network connection. Enter a user friendly name for 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, and must match the AP ESSID for the mobile computer to communicate with the AP.

NOTE   Two profiles with the same user friendly name are acceptable 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.
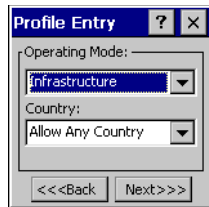
Figure 4-8   *Operating Mode Dialog Box*

Table 4-5 *Operating Mode Fields*

Field	Description
Operating Mode	Select **Infrastructure** to enable the mobile computer to transmit and receive data with an AP. Infrastructure is the default mode. 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** determines if the profile is valid for the country of operation. The profile country must match the country in the options page or it must match the acquired country if 802.11d is enabled. **Single Country Use:** When the device is only used in a single country, set every profile country to **Allow Any Country**. In the **Options** > **Regulatory** dialog box (see *Figure 4-48 on page 4-35)*, select the specific country the device is used in, and deselect the **Enable 802.11d** option. This is the most common and efficient configuration, eliminating the initialization overhead associated with acquiring a country via 802.11d. **Multiple Country Use:** When the device is used in more than one country, select the **Enable 802.11d** option in the **Options** > **Regulatory** dialog box (see *Figure 4-48 on page 4-35)*. This eliminates the need for reprogramming the country (in **Options** > **Regulatory**) each time you enter a new country. However, this only works if the infrastructure (i.e., APs) supports 802.11d (some infrastructures do not support 802.11d, including some Cisco APs). When the Enable 802.11d option is selected, the **Options** > **Regulatory** > **Country** setting is not used. For a single profile that can be used in multiple countries, with infrastructure that supports 802.11d (including Symbol 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 4-9* for instruction on setting up authentication.

Ad-Hoc

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

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

Table 4-6   *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
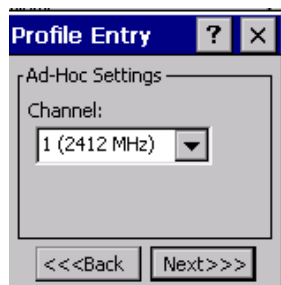
Figure 4-9   *Ad-Hoc Settings Dialog Box*

2. Tap **Next**. The **Encryption** dialog box displays. See *Encryption on page 4-16* for encryption options.

Authentication

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

Select an authentication type from the drop-down list and tap **Next**. Selecting **PEAP** or **TTLS** displays the **Tunneled** dialog box. Selecting **None**, **TLS**, or **LEAP** displays the **Encryption** dialog box. See *Encryption on page 4-16* for encryption options. *Table 4-7* lists the available authentication options.

Figure 4-10   *Authentication Dialog Box*

Table 4-7   *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 by using secure authentication certificates.
PEAP	Select this option to enable PEAP authentication. This method uses a digital certificate to verify and authenticate a user's identity.
LEAP	Select this option to enable LEAP authentication, which is based on mutual authentication. The AP and the connecting mobile computer require authentication before gaining access to the network.
TTLS	Select this option to enable TTLS authentication.

Tunneled Authentication

Use the **Tunneled Authentication** dialog box to select the tunneled authentication options. There are different selections available for PEAP or TTLS authentication.
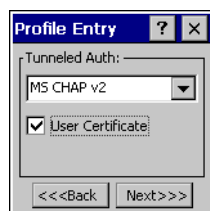
Figure 4-11   *Tunneled Authentication Dialog Box*

To select a tunneled authentication type:

1.   Select a tunneled authentication type from the drop-down list. See *Table 4-8* and *Table 4-9*.

2.   Select the **User Certificate** check box if a certificate is required. If you selected the TLS tunnel type that requires a user certificate, the check box is already selected.

3.   Tap **Next**. The **Installed User Certificates** dialog box appears.

Table 4-8 lists the PEAP tunneled authentication options.

Table 4-8   *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 phase 2 of the authentication process. This method uses a user certificate to authenticate.

Table 4-9 lists the TTLS tunneled authentication options.

Table 4-9   *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 is established.
MS CHAP	Microsoft Challenge Handshake Authentication Protocol (MS CHAP) is an implementation of the CHAP protocol that Microsoft created to authenticate remote Windows workstations. MS CHAP is identical to CHAP, except that MS CHAP is based on the encryption and hashing algorithms used by Windows networks, and the MS CHAP response to a challenge is in a format optimized for compatibility with Windows operating systems.
MS CHAP v2	MS CHAP v2 is a password based, challenge response, mutual authentication protocol that uses the industry standard Message Digest 4 (MD4) and Data Encryption Standard (DES) algorithms to encrypt responses. The authenticating server challenges the access client and the access client challenges the authenticating server. If either challenge is not correctly answered, the connection is rejected. MS CHAP v2 was originally designed by Microsoft as a PPP authentication protocol to provide better protection for dial-up and virtual private network (VPN) connections. With Windows XP SP1, Windows XP SP2, Windows Server 2003, and Windows 2000 SP4, MS CHAP v2 is also an EAP type.
PAP	Password Authentication Protocol (PAP) has two variations: PAP and CHAP PAP. It verifies a user name and password for PPP Internet connections, but it is not as secure as CHAP, since it works only to establish the initial link. PAP is also more vulnerable to attack because it sends authentication packets throughout the network. Nevertheless, PAP is more commonly used than CHAP to log in to a remote host like an Internet service provider.
MD5	Message Digest-5 (MD5) is an authentication algorithm developed by RSA. MD5 generates a 128-bit message digest using a 128-bit key, IPSec truncates the message digest to 96 bits.

User Certificate Selection

If you checked the **User Certificate** check box on the **Tunneled Authentication** dialog box or if **TLS** is the selected authentication type, the **Installed User Certificates** dialog box displays. Select a certificate from the drop-down list of currently installed certificates before proceeding. The selected certificate's name appears in the drop-down list. If the required certificate is not in the list, install it.
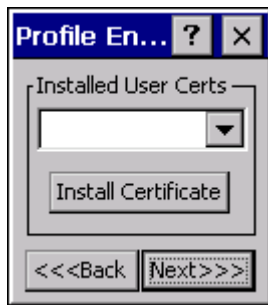
Figure 4-12   *Installed User Certificates Dialog Box*

User Certificate Installation

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

1.   Tap **Install Certificate**. The **Credentials** dialog box appears.
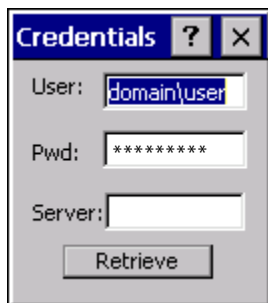
Figure 4-13   *Credentials Dialog Box*

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

3.   Tap **Retrieve**. A **Progress** dialog indicates the status of the certificate retrieval.

4.   Tap **ok** to exit.

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

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

1.   Tap the **Install Certificate** button.
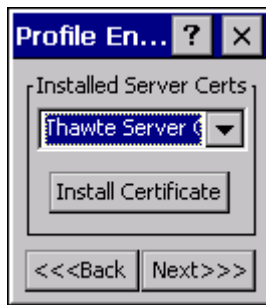
Figure 4-14   *Installed Server Certificates Dialog Box*

A dialog box appears that lists the currently loaded certificate files found in the default directory (Application directory for Windows CE and all folders for Windows Mobile) with the default extension.
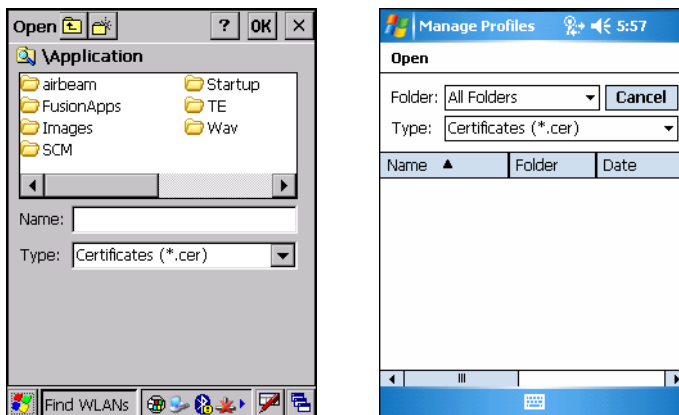
Figure 4-15   *Browse Server Certificates*

2.   Locate a certificate:

   a.   For Windows Mobile, select a different folder, if applicable, using the **Folder** drop-down list. Tap the certificate filename. The certificate installs automatically.

   b.   For Windows CE, 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.
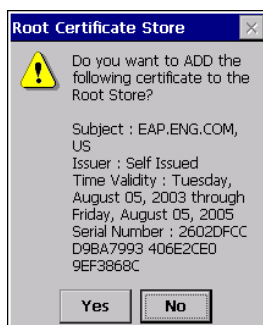
Figure 4-16   *Confirmation Dialog Box*

Credential Cache Options

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

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

Caching options only apply on credentials entered through the login dialog box.
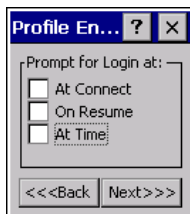
Figure 4-17   *Prompt for Login at Dialog Box*

If the mobile computer does not have the credentials, you are 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 you entered the credentials via the profile, the mobile computer does not prompt for new credentials. *Table 4-10* lists the caching options.

Table 4-10   *Cache Options*

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

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

The following authentication types have credential caching:

- EAP TLS
- PEAP
- LEAP
- TTLS.

Selecting the **At Time** check box displays the **TIme Cache Options** dialog box.
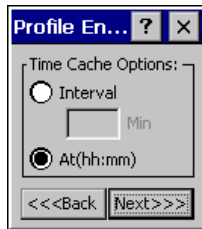
Figure 4-18   *Time Cache Options Dialog Box*

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 the **At (hh:mm)** radio button to check credentials at a set time.

4. Tap **Next**. The **At Time** dialog box appears.
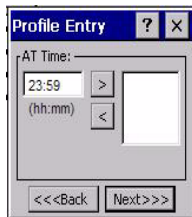
Figure 4-19   *At Time Dialog Box*

5. Enter the time using the 24 hour clock format in the **(hh:mm)** box.

6. Tap **>** to move the time to the right. Repeat for additional time periods.

7. 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.
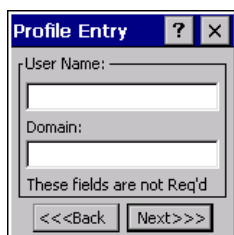
Figure 4-20   *Username Dialog Box*

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 4-21   *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 4-17*.

Advanced Identity

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

> **NOTE**   When authenticating with a Microsoft IAS server, do not use advanced identity.
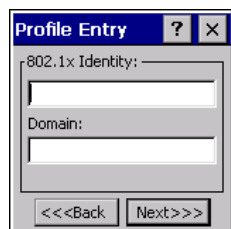
Figure 4-22   *Advanced Identity Dialog Box*

Tap **Next**. The **Encryption** dialog box displays.

Encryption

Use the **Encryption** dialog box to select an encryption type. The drop-down list includes encryption types available for the selected authentication type. See *Table 4-12* for these encryption types.

Figure 4-23   *Encryption Dialog Box*

Table 4-11   *Encryption Options*

Encryption	Description
Open	Select *Open* (the default) when no data packet encryption is needed over the network. Selecting this option provides no security for data transmitting over the network.
40-Bit WEP	Select 40-Bit WEP to use 40-bit key length WEP encryption. WEP keys are manually entered in the edit boxes. Only the required number of edit boxes for a key length is displayed (10 Hex digit value for 40-bit keys). Use the *Key Index* drop-down list to configure the four WEP keys. The adapter uses the selected key. Note: The default Hex digit keys are visible any time they are used. As a security precaution after setting the key values for the network, the digits are replaced with asterisks * in the encryption key fields. If the associated AP uses an optional passkey, the active adapter WLAN profile must use one as well. The passkey is a plain text representation of the WEP keys displayed in the encryption dialog box. The passkey provides an easy way to enter WEP key data without having to remember the entire 40-bit (10 character) Hex digit string.
128-Bit WEP	Select 128-Bit WEP to use 128-bit key length WEP encryption. WEP keys are manually entered in the edit boxes. Only the required number of edit boxes for a key length is displayed (26 Hex digit value for 128-bit keys). Use the *Key Index* drop-down list to configure the four WEP keys. The adapter uses the selected key. Note: The default Hex digit keys are visible any time they are used. As a security precaution after setting the key values for the network, the digits are replaced with asterisks * in the encryption key fields. If the associated AP uses an optional passkey, the active adapter WLAN profile must use one as well. The passkey is a plain text representation of the WEP keys displayed in the encryption dialog box. The passkey provides an easy way to enter WEP key data without having to remember the entire 128-bit (26 character) Hex digit string.
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 4-12   *Encryption / Authentication Matrix*

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

Key Entry Page

If you select either **40-Bit WEP** or **128-Bit WEP** the wizard proceeds to the key entry dialog box unless the **Use Passkey** check box was selected in the **Encryption** dialog box (see *Figure 4-23 on page 4-16*). 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**.
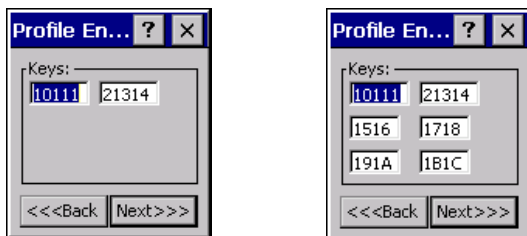
40-Bit WEP Keys Dialog Box   128-Bit WEP Keys Dialog Box

Figure 4-24   *40-Bit and 128-Bit WEP Keys Dialog Boxes*

Passkey Dialog

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

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

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

Figure 4-25   *Passkey Dialog Box*

Tap **Next**. The **IP Address Entry** dialog box displays.

IP Address Entry

Use the **IP Address Entry** dialog box to configure network address parameters: IP address, subnet, gateway, DNS, and WINS.
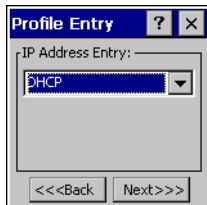
Figure 4-26   *IP Address Entry Dialog Box*

Table 4-13   *IP Address Entry*

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

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

Use the **IP Address Entry** dialog box to enter the IP address and subnet information.
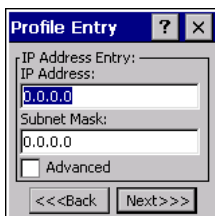
Figure 4-27   *Static IP Address Entry Dialog Box*

Table 4-14   *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 to manage routed IP addresses. Dividing an organization's network into subnets allows it to connect to the Internet with a single shared network address, for example, 255.255.255.0.

Select the **Advanced** check box, then tap **NEXT** to display the **Advanced Address Entry** dialog box. Enter the Gateway, DNS, and WINS address. Tap **NEXT** without selecting the **Advanced** check box to display the **Transmit Power** dialog box.
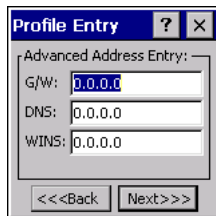
Figure 4-28 *Advanced Address Entry Dialog Box*

The IP information entered in the profile is only used if you selected the **Enable IP Mgmt** check box in the **Options** > **System Options** dialog box (*System Options on page 4-35*). If you didn't select this, the IP information in the profile is ignored and the IP information entered in the Microsoft interface applies.

Table 4-15 *IP Config Advanced Address Entry Fields*

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

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

Transmit Power

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

Adjusting the radio transmission power level enables the user to expand or confine the transmission area with respect to other wireless devices that could be operating nearby. Reducing coverage in high traffic areas improves transmission quality by reducing the amount of interference in that coverage area.
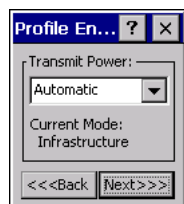
Figure 4-29 *Transmit Power Dialog Box (Infrastructure Mode)*

Table 4-16 *Transmit Power Dialog Box (Infrastructure Mode)*

Field	Description
Automatic	Select **Automatic** (the default) to use the AP power level.
Power Plus	Select **Power Plus** to set the mobile computer transmission power one level higher than the level set for the AP.
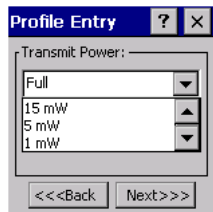
Figure 4-30 *Transmit Power Dialog Box (Ad-Hoc Mode)*

Table 4-17 *Power Transmit Options (Ad-Hoc Mode)*

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

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

Battery Usage

Use the **Battery Usage** dialog box to select power consumption of the wireless LAN. There are three settings available: CAM, Fast Power Save, and MAX Power Save. Battery usage cannot be configured in Ad-Hoc profiles.
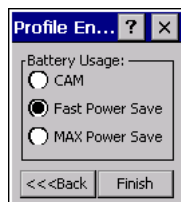
Figure 4-31 *Battery Usage Dialog Box*

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

Table 4-18   *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** (the default) performs in the middle of CAM and MAX Power Save with respect to network performance and battery life.
MAX Power Save	**Max Power Save** yields the longest battery life while potentially reducing network performance. In networks with minimal latency, Max Power Save performs as well as Fast Power Save, but with increased battery conservation.

Manage Profiles Application

The **Manage Profiles** window provides a list of user-configured wireless profiles. Define up to 32 profiles at any one time. To open the **Manage Profiles** window, tap the **Signal Strength** icon > **Manage Profiles**.
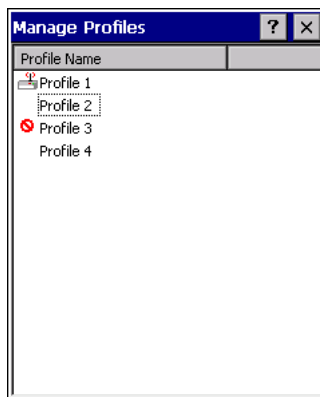
Figure 4-32   *Manage Profiles Window*

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

Table 4-19   *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 in use and describes an infrastructure profile not using encryption.
	Profile is in use and describes an infrastructure profile using encryption.

Table 4-19 *Profile Icons (Continued)*

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

The profiles are listed in priority order for use by the automatic roaming feature. Change the order by moving profiles up or down. To edit existing profiles, tap and hold one in the list and select an option from the menu to connect, edit, disable (enable), or delete the profile. (Note that the *Disable* menu item changes to *Enable* if the profile is already disabled.)
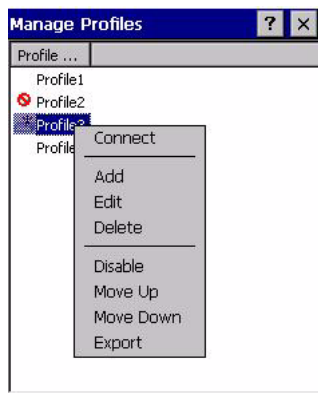
Figure 4-33 *Manage Profiles Context Menu*

Changing Profiles

A completed profile is a set of configuration settings that can be used in different locations to connect to a wireless network. Create different profiles to have pre-defined operating parameters available for use in various network environments. When the **WLAN Profiles** window displays, existing profiles appear in the list.
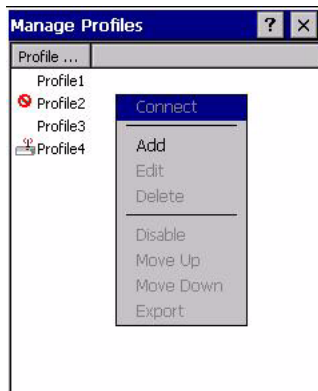
Figure 4-34 *Manage Profiles*

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

Editing a Profile

Tap and hold a profile and select **Edit** from the pop-up menu to display the **Profile Wizard** where you can set the ESSID and operating mode for the profile. Use the **Profile Wizard** to edit the profile power consumption and security parameters. *See Profile Editor Wizard on page 4-6.*

Creating a New Profile

To create new profiles from the **Manage Profiles** window, tap-and-hold anywhere in this window.
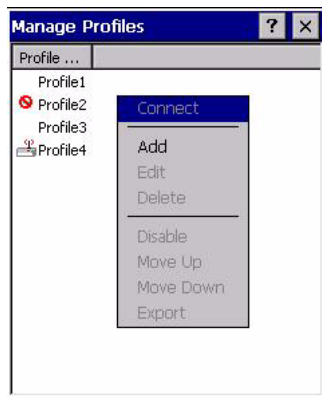
Figure 4-35   *Manage Profiles - Add*

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

Deleting a Profile

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

Ordering Profiles

Tap and hold a profile from the list and select **Move Up or Move Down** to order the profile. If the current profile association is lost, the mobile computer attempts to associate with the first profile in the list, then the next, until it achieves a new association.

NOTE   Profile Roaming must be enabled.

Export a Profile

To export a profile to a registry file, tap and hold 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).
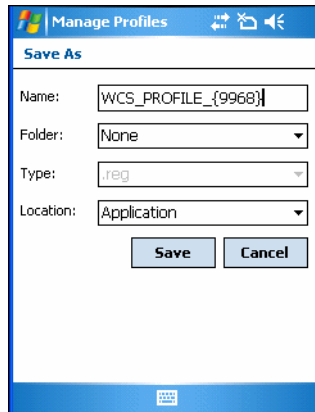
Figure 4-36 *Save As Dialog Box*

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

Wireless Status Application

To open the **Wireless Status** window, tap the **Signal Strength** icon > **Wireless Status**. The **Wireless Status** window displays information about the wireless connection.
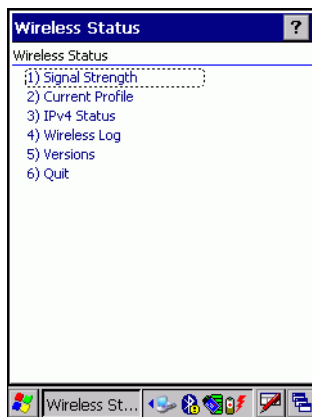
Figure 4-37 *Wireless Status Window*

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

To open the **Signal Status** window, tap **Signal Strength** in the **Wireless Status** window.
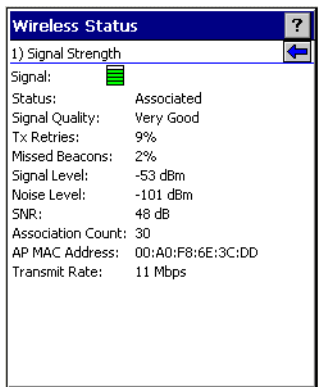
Figure 4-38   *Signal Strength Window*

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

Table 4-20   *Signal Strength Status*

Field	Description
Signal	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.
	![icon] Excellent Signal
	![icon] Very Good Signal
	![icon] Good Signal
	![icon] Fair Signal
	![icon] Poor Signal
	![icon] Out of Range (no signal)
	![icon] The radio card is off or there is a problem communicating with the radio card.
Status	Indicates if the mobile computer is associated with the AP.
Signal Quality	Displays a text format of the Signal icon.
Tx Retries	Displays a percentage of the number of data packets the mobile computer retransmits. The fewer transmit retries, the more efficient the wireless network is.

Table 4-20 *Signal Strength Status (Continued)*

Field	Description
Missed Beacons	Displays a percentage of the amount of beacons the mobile computer missed. The fewer transmit retries, the more efficient the wireless network is. Beacons are uniform system packets broadcast by the AP to keep the network synchronized.
Signal Level	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).
Association Count	Displays the number of APs the mobile computer connects to while roaming.
AP MAC Address	Displays the MAC address of the AP to which the mobile computer is connected.
Transmit Rate	Displays the current rate of the data transmission.

Current Profile Window

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

To open the **Current Profile** window, tap **Current Profile** in the **Wireless Status** window.
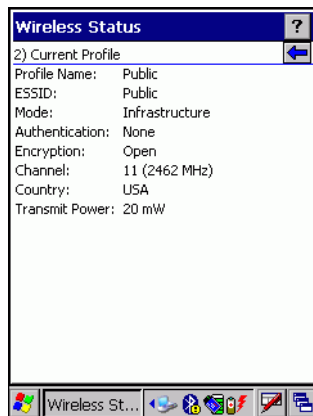
Figure 4-39 *Current Profile Window*

Table 4-21 *Current Profile Window*

Field	Description
Profile Name	Displays the current profile name the mobile computer uses to communicate with the AP.
ESSID	Displays the current profile ESSID name.
Mode	Displays the current profile mode, either Infrastructure or Ad-Hoc.
Authentication	Displays the current profile's authentication type.
Encryption	Displays the current profile's encryption type.

Table 4-21 *Current Profile Window*

Field	Description
Channel	Displays the current profile's channel setting.
Country	Displays the current profile's country setting.
Transmit Power	Displays the radio transmission power level.

IPv4 Status Window

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

To open the **IPv4 Status** window, tap **IPv4 Status** in the **Wireless Status** window.
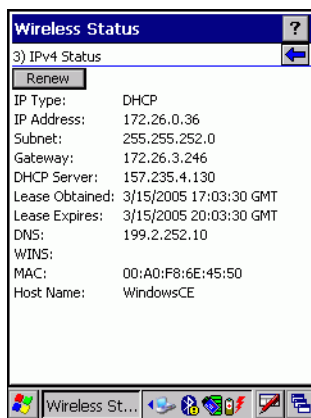
Figure 4-40 *IPv4 Status Window*

Table 4-22 *IPv4 Status Fields*

Field	Description
IP Type	Displays the IP type for the current profile: **DHCP** or **Static**. If the IP type is DHCP, leased IP address and network address data appear for the mobile computer. If the IP type is Static, the values displayed were input manually in the **IP Config** tab on page 4-19.
IP Address	Displays the mobile computer's IP address. The Internet is a collection of networks with users that communicate with each other. Each communication carries the address of the source and destination networks and the particular machine within the network associated with the user or host computer at each end. This address is called the IP address. Each node on the IP network must be assigned a unique IP address that is made up of a network identifier and a host identifier. The IP address as a dotted-decimal notation with the decimal value of each octet separated by a period, for example, 192.168.7.27.
Subnet	Displays the subnet address. Most TCP/IP networks use subnets to manage routed IP addresses. Dividing an organization's network into subnets allows it to connect to the Internet with a single shared network address, for example, 255.255.255.0.
Gateway	Displays the gateway address. A gateway forwards IP packets to and from a remote destination.

Table 4-22   *IPv4 Status Fields (Continued)*

Field	Description
DCHP Server	The Domain Name System (DNS) is a distributed Internet directory service. DNS translates domain names and IP addresses, and controls Internet e-mail delivery. Most Internet services require DNS to operate properly. If DNS is not configured, Web sites cannot be located or e-mail delivery fails.
Lease Obtained	Displays the date that the IP address was obtained.
Lease Expires	Displays the date that the IP address expires and a new IP address is requested.
DNS	Displays the IP address of the DNS server.
WINS	WINS is a Microsoft Net BIOS name server. WINS eliminates the broadcasts needed to resolve computer names to IP addresses by providing a cache or database of translations.
MAC	An IEEE 48-bit address is assigned to the mobile computer at the factory to uniquely identify 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 recent activity, such as authentication, association, and DHCP renewal completion, in time order. Save the log to a file or clear the log (within this instance of the application only). The auto-scroll feature automatically scrolls down when new items are added to the log.

To open the **Wireless Log** window, tap **Wireless Log** in the **Wireless Status** window. The **Wireless Log** window displays.
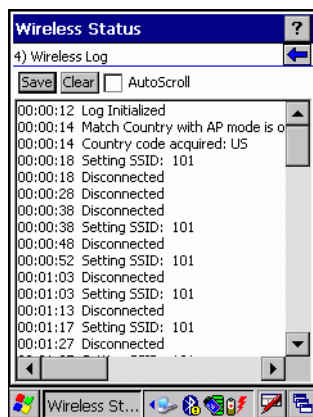
Figure 4-41   *Wireless Log Window*

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.

Clearing the Log

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

Versions Window

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

To open the **Versions** window, tap **Versions** in the **Wireless Status** window.
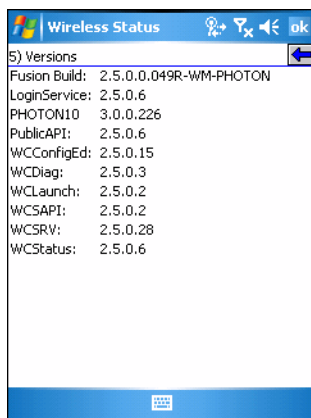
Figure 4-42   *Versions Window*

The window displays software version numbers for the following:

- Configuration Editor (Fusion 2.4 and lower only)
- Fusion Build
- LoginService
- PublicAPI (Fusion 2.5 and higher only)
- Photon10
- WCConfigED
- WCDiag
- 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**.
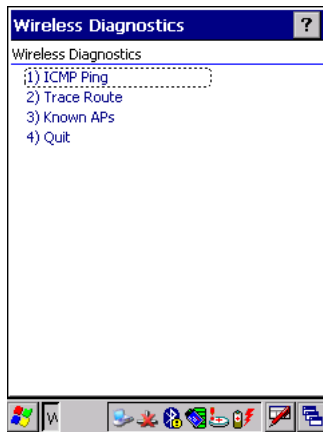
Figure 4-43   *Wireless Diagnostics Window*

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 **Wireless Diagnostics** window.

ICMP Ping Window

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

To open the **ICMP Ping** window, tap **ICMP Ping** in the **Wireless Diagnostics** window.
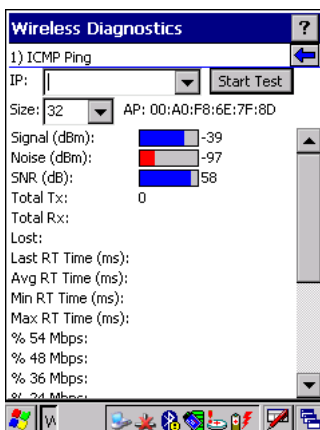
Figure 4-44   *ICMP Ping Window*

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 occur.

The **Trace Route** window allows testing 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.
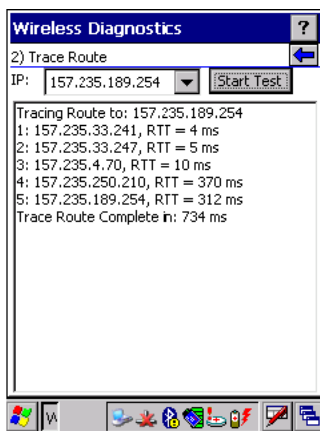
Figure 4-45   *Trace Route Window*

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

Known APs Window

The **Known APs** window displays the APs in range using the same ESSID as the mobile computer. This window is only available in **Infrastructure** mode. To open the **Known APs** window, tap **Known APs** in the **Wireless Diagnostics** window.
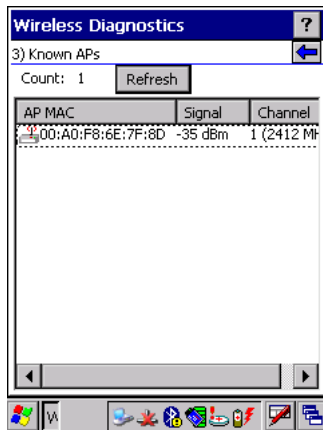
Figure 4-46   *Known APs Window*

See *Table 4-23* for the definitions of the icons next to the AP.

Table 4-23   *Current Profile Window*

Icon	Description
	The AP is the associated access point, and is set to mandatory.
	The AP is the associated access point, but is not set to mandatory.
	The mobile computer is not associated to this AP, but the AP is set as mandatory.
	The mobile computer is not associated to this AP, and AP is not set as mandatory.

Tap and hold on an AP to display a pop-up menu with the following options: **Set Mandatory** and **Set Roaming**.

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

- You select **Set Roaming**
- The mobile computer roams to a new profile
- The mobile computer suspends
- The mobile computer resets (warm or cold).

Select **Set Roaming** to allow 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. The highest signal strength value is 32.

Options

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

- Operating Mode Filtering
- Regulatory
- Band Selection

- System Options

- Change Password

- Export.

Operating Mode Filtering

The **Operating Mode Filtering** options cause the Find WLANs application to filter the available networks found.
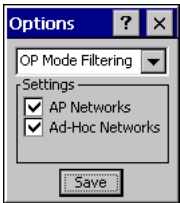
Figure 4-47 *OP Mode Filtering Dialog Box*

The **AP Networks** and **Ad-Hoc Networks** check boxes are selected by default.

Table 4-24 *OP Mode Filtering Options*

Field	Description
AP Networks	Select the **AP Networks** check box to display available AP networks and their signal strength within the **Available WLAN Networks** (see *Find WLANs Application on page 4-5*). These are the APs available to the 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.
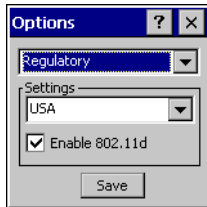
Figure 4-48   *Regulatory Options Dialog Box*

Table 4-25   *Regulatory Options*

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

Band Selection

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

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

Figure 4-49   *Band Selection Dialog Box*

Table 4-26   *Band Selection Options*

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

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

System Options

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

Figure 4-50   *System Options Dialog Box*

Table 4-27   *System Options*

Field	Description
Profile Roaming	Configures 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	Enables the Wireless Companion Services to handle IP address management. The Wireless Companion Service configures the IP based on what is configured in the network profile. Deselect this to manually configure the IP in the standard Windows IP window. Enabled by default.
Auto Time Config	Enables automatic update of the system time. Network association updates the device time based on the time set in the AP. This proprietary feature is only supported with Symbol infrastructure. Enabled by default.

Change Password

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

Figure 4-51   *Change Password Window*

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**.

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

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

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

Export

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

Figure 4-52 *Options - Export Dialog Box*

To export options:

1. Tap **Export Options**. The **Save As** dialog box displays.
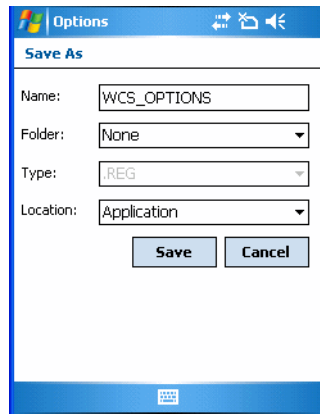
Figure 4-53 *Export Options Save As Dialog Box*

2. Enter a filename in the **Name:** field. The default filename is WCS_OPTIONS.REG.

3. Tap **Save**.

To export all profiles:

1. Tap **Export All Profiles**. The **Save As** dialog box displays.
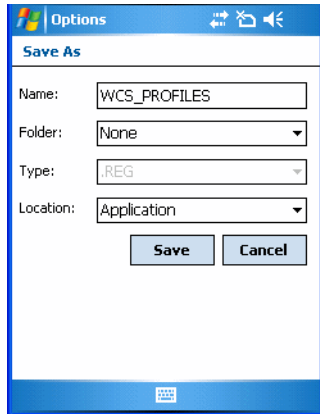
Figure 4-54   *Export All Profiles Save As Dialog Box*

2.   Enter a filename in the **Name:** field. The default filename is WCS_PROFILES.REG.

3.   In the **Folder:** drop-down list, select the desired folder.

4.   Tap **Save**.

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

Persistence

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

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

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

Registry Settings

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

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

Table 4-28   *Registry Parameter Settings*

Key	Type	Default	Description
CertificateDirectory	REG_SZ	\\Applications	The default directory to find certificates.
EncryptionMask	REG_DWORD	0x0000001F	Defines the supported encryption types. This is a bitwise mask with each bit corresponding to an encryption type. 1 = Type is supported 0 = Type is not supported Bit Number Encryption Type 0 None 1 40-Bit WEP 2 128-Bit WEP 3 TKIP 4 AES (Fusion 2.5 and higher only)

Log On/Off Application

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

User Already Logged In

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

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

> *NOTE* Re-enable cancelled profiles using the Profile Editor Wizard and choosing to connect to the cancelled profile. Cancelled profiles are also re-enabled when a new user logs on.

- Log off the 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

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

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

- Launched by WCS, because the service is connecting to a new profile that needs credentials.

- Launched by WCS, because the service is trying to verify the credentials due to credential caching rules.

- Launched by a user, when a user is logged in.

- Launched by a user, when no user is logged in.

Table 4-29 *Log On/Off Options*

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

Table 4-29   *Log On/Off Options (Continued)*

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

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 5 MC9094 Configuration

Introduction

This chapter explains how to verify MC9094 service on an Enhanced Data rates for Global Evolution (EDGE) wireless network and establish settings. EDGE is also known as Enhanced General Packet Radio Service (EGPRS).

EDGE networks deliver mobile voice and data services, such as Short Message Service (SMS)/Text Messaging, with full roaming capabilities across the world. General Packet Radio Service (GPRS) enabled networks offer Internet-based content and packet-based data services. This enables services such as internet browsing, e-mail on the move, powerful visual communications, multimedia messages and location-based services.

When using the MC9094 as a phone, services can include speed dialing, call tracking, voice mail, call forwarding, conference calling and caller ID, depending on the type of service.

The integrated phone in the mobile computer can also be used as a modem to connect the mobile computer to an ISP or work network. The GSM/GPRS enabled mobile computer can connect to the Internet or work network over GPRS, using Cellular Line, or using the modem specified by the mobile phone service provider.

✓ **NOTE**	Before a mobile computer can be used on a wireless network, a provider must be selected, a voice and data-enabled service plan must be established and the mobile computer must be properly configured (where applicable).

Refer to the *MC909X User Guide* for information on how to use the phone and services.

Quick Startup Steps

To start using the MC9094 mobile computer for phone and data connections:

1. Install the mobile computer main battery. See *Installing and Removing the Main Battery on page 1-6* for more information.

2. Charge the main battery and backup battery. See *Charging the Battery on page 1-7* for more information.

3. Install the SIM card. See *SIM Card on page 1-14* for more information.

4. Start the mobile computer.

5. Ensure network coverage (*Ensuring Network Coverage on page 5-2*).

6. Configure an GPRS data connection (*Configuring an GPRS Data Connection on page 5-3*).

7. Configure settings (*Phone Settings on page 5-7*).

8. Use the phone.

MC9094 Service Verification

MC9094 phone and data services require a live SIM card, obtained from a service provider, installed in the MC9094 phone/mobile computer. The SIM card has embedded circuitry on one side of its surface which, when inserted into a MC9094 phone, provides phone service on an EDGE/GPRS network. The SIM card provides a phone number, determines the features or services available to the subscriber and identifies the subscriber to the network.

In addition to SIM card installation, various settings may be required for the mobile computer to operate as a phone with data connection features.

When connected to a GRPS network, the icons appears in the Status Bar and when connected to an EDGE network the icon appears in the status bar.

Ensuring Network Coverage

1. Ensure an activated SIM card, from the phone service provider, is installed in the mobile computer.

> *NOTE*   The SIM card must be EDGE/GPRS enabled to connect to a EDGE/GPRS network.

2. Verify active phone and data services by tapping to display the **Phone** dialog. The network service provider name appears in the dialog box.
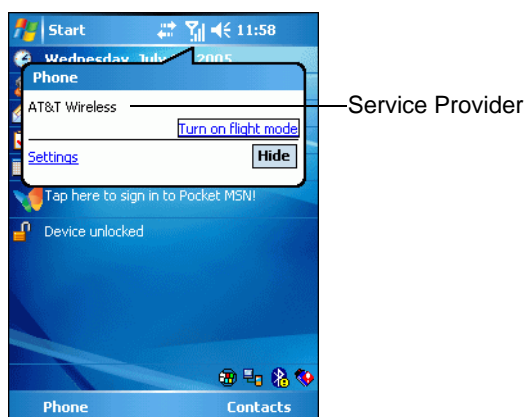
Figure 5-1   *Connectivity Dialog*

3. Verify SIM card functionality.

   a.   Tap **Start** > **Settings** > **Phone** icon > **Network** tab.
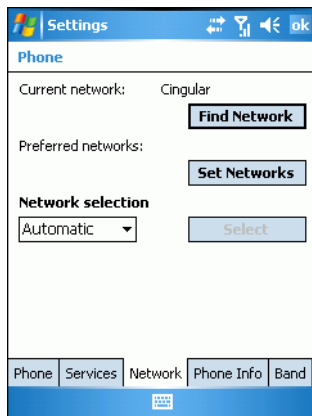
Figure 5-2   *Phone Settings Window - Network Tab*

      b.   Ensure the service provider's network appears in the **Current network:** field.

4.   If the network does not appear, tap **Find Network**. If the network still does not appear, verify that the SIM card was installed correctly. If it was, and no network appears, contact the service provider.

Configuring an GPRS Data Connection

An GPRS data connection allows Internet access across a wireless network.

To set up a new data connection:

1.   Acquire an Access Point Name (APN) from the service provider.

2.   Tap **Start** > **Settings** > **Connections** tab > **Connections** icon > **Tasks** tab.
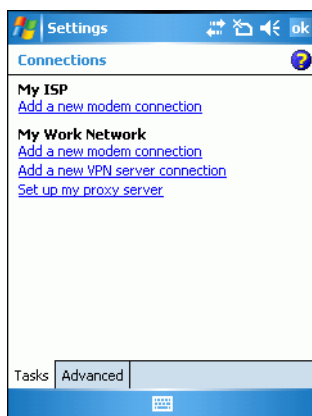
Figure 5-3   *Connections Window*

3.   Under **My ISP** select **Add a new modem connection**.
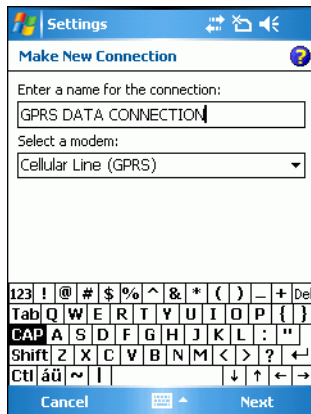
Figure 5-4   *Connections Window - Make New Connection*

4.   Enter a connection name in the **Enter a name for the connection:** text box.

5.   Select **Cellular Line (GPRS)** from the **Select a modem:** drop-down list.

6.   Tap **Next**.
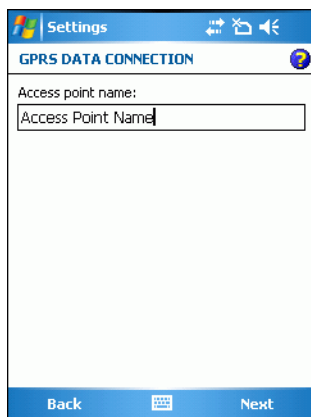
Figure 5-5   *Connections Window - Access Point Name*

7.   Enter the APN from the service provider in the **Access point name:** text box.

8.   Tap **Next**.
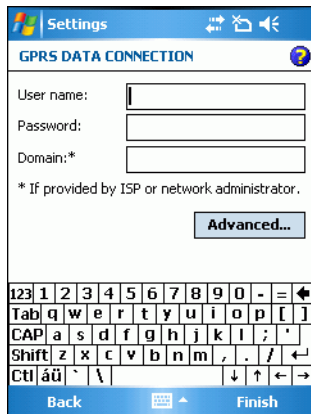
Figure 5-6   *Connections Window - User Name & Password*

9.   Tap **Finish** (user name and password are not required).

10.   Tap **ok** to exit **Connections**.

Establishing a Data Connection

1.   Ensure a SIM card is installed in the mobile computer.

2.   Ensure an GPRS data connection was configured. See *Configuring an GPRS Data Connection on page 5-5*.

3.   Tap   at the top of the screen.
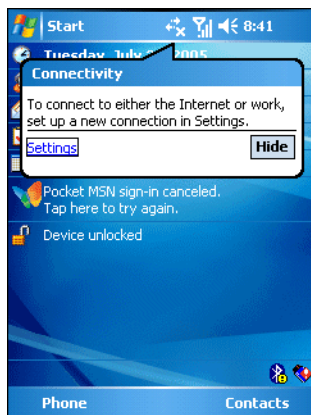
Figure 5-7   *Connectivity Dialog*

4.   Tap **Settings**.

5.   Tap **Managing existing connections**.

6.   Tap and hold on the data connection until a menu appears.
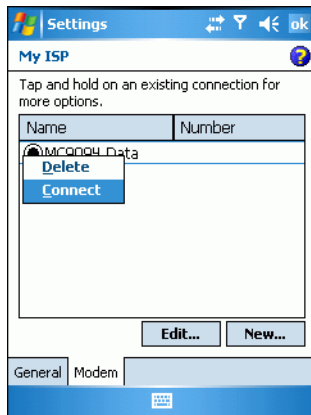
Figure 5-8   *Data Connection*

7.   Select **Connect**.
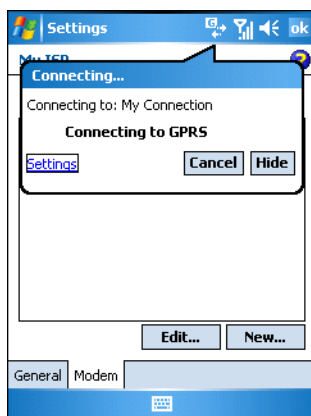
Figure 5-9   *Connecting Using GPRS Packet Data Modem*

8.   If the SIM card is protected with a Personal Identification Number (PIN), a dialog box pops up requesting the appropriate PIN to unlock the SIM card. In this case, enter the PIN and tap **ok**.

> *NOTE*   Emergency calls can be placed at any time, without requiring a PIN or a SIM card.

9.   When a connection is established, launch **Internet Explorer** to browse the Internet or launch an applicable application.

Ending an GPRS Data Connection

To cancel a data connection in progress, tap **Cancel** in the **Connecting...** dialog window.

To end an established data connection:

1.   Tap [icon] to display the dialog window.
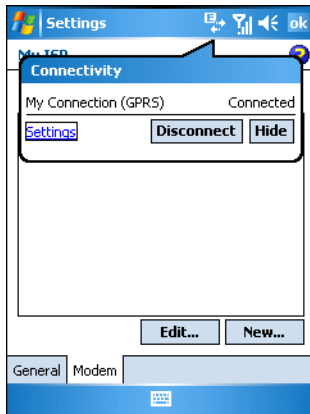
Figure 5-10   *Connectivity Dialog Box*

2.   Tap **Disconnect**.

> *NOTE*   When **Disconnect** is tapped during an active data transfer (e.g., downloading a web page), the GPRS connection automatically reconnects. The GPRS connection cannot be disconnected until the data transfer is complete.

Phone Settings

Use the **Phone Settings** window to customize settings, such as the ring type and ring tone for incoming calls, security options (GPRS) and other options depending on the type of service.

Phone

Use the *Phone* tab to customize ring type, ring tone, keypad tone and security options.

Tap **Start** > **Settings** > **Personal** tab > **Phone** icon > **Phone** tab.

or

Start > **Phone** > **Menu** > **Options** > **Phone** tab.
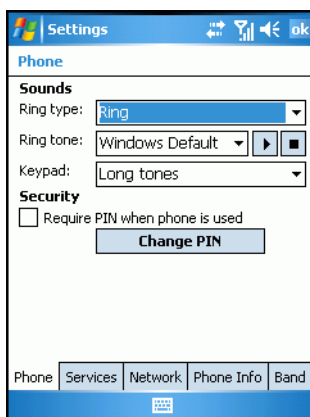
Figure 5-11   *MC9094 Phone Window - Phone Tab*

Sounds

1. **Phone Number** automatically displays on the **Phone** tab when a live SIM card is installed.

2. Select a ring type from the **Ring type:** drop-down list. The ring type changes the way the mobile computer rings to notify the user of an incoming call. Regardless of the ring type selected, a dialog box appears on the mobile computer's display for incoming calls.

3. Select a ring tone for incoming calls from the **Ring tone:** drop-down list. To hear a sample of the selected ring tone, tap ▶ . Tap ■ to end the ring tone.

> *NOTE*   To use custom .wav, .mid or .wma files as ring tones, use ActiveSync on the host computer to copy the file to the /Windows/Rings folder on the mobile computer. Then, select the sound from the ring tone list.

4. Select a keypad tone from the **Keypad:** drop-down list. This selection determines the tone that sounds when entering a phone number on the keypad.

    a. Select **Tones** for a continuous sound for as long as the number on the keypad is pressed.

    b. Select **Beep** for a tone that sounds only for one or two seconds.

    c. Select **Off** to disable tones.

5. Tap **Other Settings...** to set additional sounds and notifications for the mobile computer.

> *NOTE*   Turning off sounds saves power and prolongs battery life.

Security

> *NOTE*   PIN Emergency calls can be placed at any time, without requiring a PIN or a SIM card.

To require a PIN when using the phone:

1. From the **Phone** tab (*Figure 5-11 on page 5-7*), select the **Require PIN when phone is used** check box under **Security**.
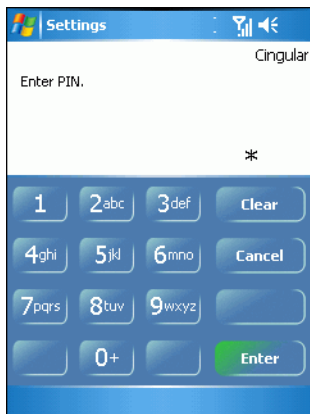
Figure 5-12   *Enter PIN*

2. Use the touch keypad to enter a four to eight digit PIN.

3. Tap **Enter** to enable the PIN and return to the **Phone** tab.

Changing a PIN

⚠️ **CAUTION**   If you enter an incorrect PIN, the message 'SIM PIN incorrect: Try again' appears. After three consecutive incorrect attempts, the SIM card is blocked. The phone does not allow you to attempt to enter your PIN again and you must obtain a PIN Unblock Key from your service provider.

1. From the **Phone** tab (*Figure 5-11 on page 5-7*), tap **Change PIN**.

2. Use the touch keypad to enter the current PIN.

3. Tap **Enter**.

4. Use the touch keypad to enter a new four to eight digit PIN.

5. Tap **Enter**.

6. Reenter the new PIN for confirmation and tap **Enter**.

7. Tap **ok** to confirm the change.

Disabling a PIN

1. From the **Phone** tab (*Figure 5-11 on page 5-7*), deselect the **Require PIN when phone is used** check box.

2. Use the touch keypad to enter the current PIN.

3. Tap **Enter**.

4. Tap **ok** to confirm the change.

5. Tap **ok** to exit settings.

Services

✓ **NOTE**   Not all services are available on all network. Contact your service provider for details.

Use the **Services** tab to configure settings for subscribed phone services. For example, block certain types of incoming and/or outgoing calls (*Call Barring (Call Blocking) on page 5-10*), allow the caller's identity to be disclosed when making outgoing calls (*Caller ID on page 5-10*), forward incoming calls to a different phone number (*Call Forwarding on page 5-11*), be notified of incoming calls when a phone session is in use (*Call Waiting on page 5-11*) and set up voice mail and short message service (*Voice Mail and Short Message Service (SMS) on page 5-12*).

1. Tap **Start** > **Settings** > **Personal** tab > **Phone** icon > **Services** tab.

    or

    Start > **Phone** > **Menu** > **Options** > **Services** tab.
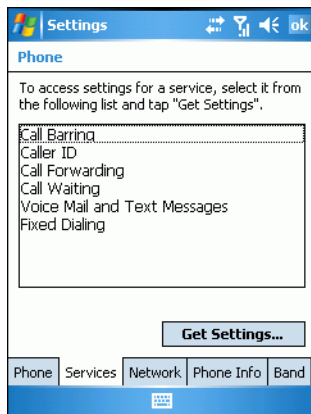
Figure 5-13   *MC9094 Phone Window - Services Tab*

2.   Select a service from the list and tap **Get Settings...** .

3.   Change services settings as follows.

Call Barring (Call Blocking)

Use call barring to block certain types of incoming and/or outgoing calls. Select the type of incoming and/or outgoing calls to block.
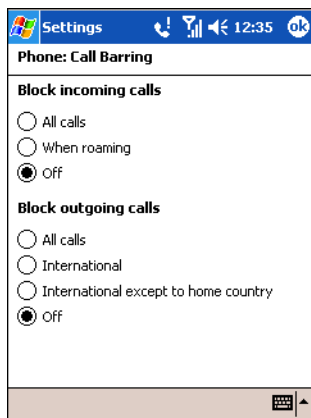
Figure 5-14   *Call Barring/Call Blocking*

Caller ID

Enable caller ID to provide a way for people to know the identity of the person making an outgoing call. Select the **Everyone** radio button to always display the caller ID. Select the **No one** radio button to prevent the caller's identity from displaying to others.
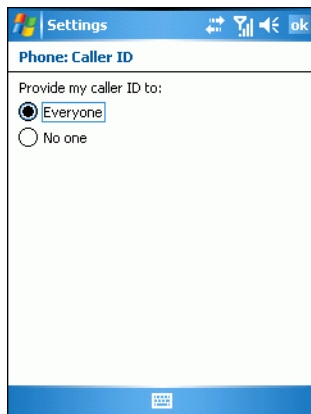
Figure 5-15   *Caller ID*

Call Forwarding

Use call forwarding to forward incoming calls to a different phone number.

- To forward all calls to a different phone number:
  - select the **Forward all incoming phone calls** check box.
  - enter the phone number to receive forwarded calls in the **To:** text box.
- To forward incoming calls to a different phone number based on a specific situation, select one or more of the check boxes under **Forward phone calls only if:**
  - **Unavailable:** enter the phone number to receive forwarded calls only when the phone is turned off or the user is unreachable.
  - **Busy:** enter the phone number to receive forwarded calls only when the line is busy.
  - **No answer:** enter the phone number to receive forwarded calls only when the phone cannot be answered.

Figure 5-16   *Call Forwarding*

Call Waiting

Call waiting notifies the user of an incoming call when the phone is in a phone session. Select the **Notify me** radio button to enable call waiting. Select the **Do not notify me** radio button to disable call waiting.
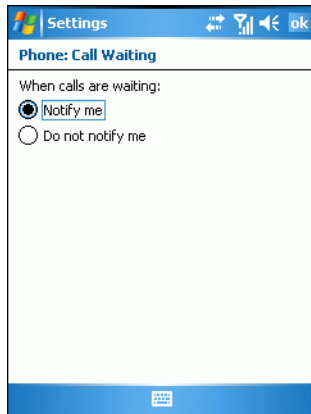
Figure 5-17   *Call Waiting*

Voice Mail and Short Message Service (SMS)

To receive voice mail and short messages, enter the voice mail and/or SMS phone number in the appropriate text boxes.
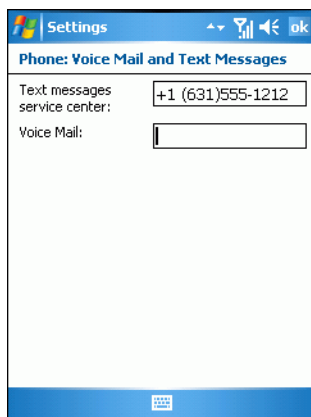
Figure 5-18   *Voice Mail and SMS*

Fixed Dialing

Use Fixed Dialing to restrict your phone to dial only the phone number(s) or area code(s) that is specified in a Fixed Dialing list.

1.   Select **Fixed Dialing** and tap **Get Settings**.
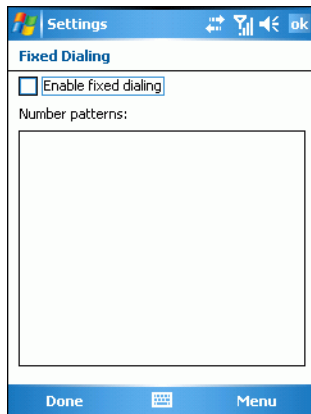
Figure 5-19   *Fixed Dialing Window*

2. Select **Enable fixed dialing**.

3. To add a number to the list, tap **Menu** > **Add**.

4. Enter the phone number or area code you want to be restricted and tap **Done**.

5. Repeat steps 3 and 4 to add more numbers, and tap **Done** twice when completed.

6. Enter **PIN2** and tap **Done**.

Network

Use the **Network** tab to view available networks, determine the order in which the phone accesses another network if the current network is unavailable and specify whether to change networks manually or automatically. The current network remains active until it's changed, the signal is lost or the SIM card is changed.

The network currently used by the mobile computer is displayed in the **Current network:** field at the top of the window.

Changing Networks Manually

1. Tap **Start** > **Settings** > **Personal** tab > **Phone** icon > **Network** tab.

    or

    Start > **Phone** > **Menu** > **Options** > **Network** tab.
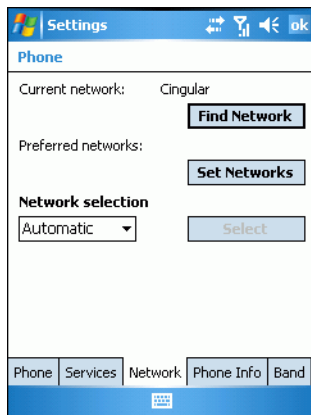
Figure 5-20   *MC9094 Phone Window - Network Tab*

2.   In the **Network selection** drop-down list, select **Manual**.
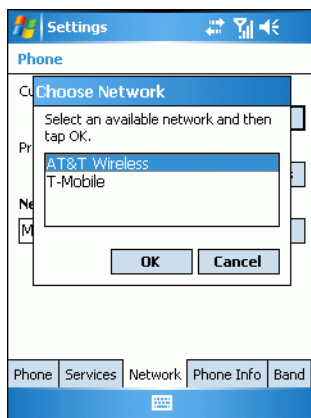
Figure 5-21   *Choose Network Dialog Box*

3.   From the **Choose Network** dialog box, select the network to use.

4.   Tap **OK**.

Viewing Available Networks

To view all wireless networks available:

1.   Tap **Start** > **Settings** > **Personal** tab > **Phone** icon > **Network** tab.

    or

    Start > **Phone** > **Menu** > **Options** > **Network** tab.
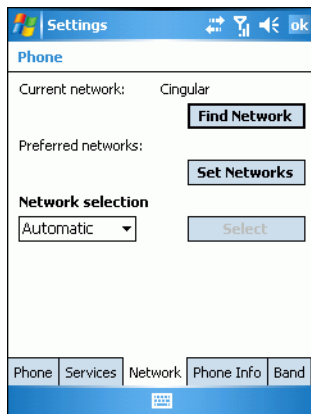
Figure 5-22   *MC9094 Phone Window - Network Tab*

2.   Tap **Find Network**.
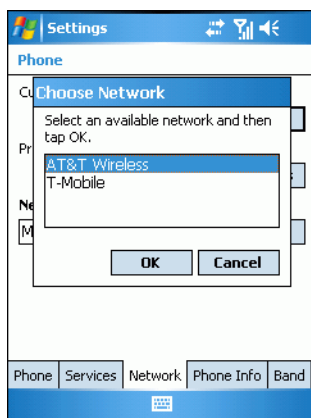
Figure 5-23   *Choose Network Dialog Box*

3.   From the **Choose Network** window, select the network to use.

4.   Tap **OK**.

Setting Preferred Networks

Set networks in a preferred order of access. Setting preferred networks allows the mobile computer to access a second preferred network if the first preferred network is unavailable.

1.   Tap **Start** > **Settings** > **Personal** tab > **Phone** icon > **Network** tab.

     or

     Start > **Phone** > **Menu** > **Options** > **Network** tab.
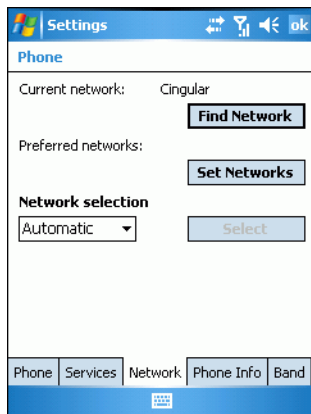
Figure 5-24   *MC9094 Phone Window - Network Tab*

2.   Tap **Set Networks** to view all available networks.
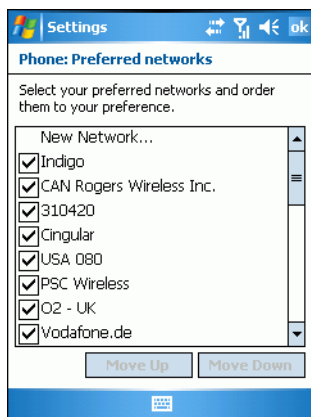
Figure 5-25   *Preferred Networks*

3.   Select the preferred networks by tapping one or more check boxes.

4.   Tap **Move Up** and **Move Down**, as necessary, to place the selected networks in the preferred order.

5.   Tap **ok** to send the new settings to the network.

6.   In the **Network Selection** drop-down list, select **Automatic**.

7.   Tap **ok** to exit settings.

Phone Info

> ![NOTE] **NOTE**   You must have a SIM Card installed to access the **Phone Info** tab.

Use the **Phone Info** tab to view hardware and software information about the phone.

1.   Tap **Start** > **Settings** > **Personal** tab > **Phone** icon > **Phone Info** tab.

   or

   Start > **Phone** > **Menu** > **Options** > **Phone Info** tab.

Figure 5-26   *MC9094 Phone Window - Phone Info Tab*

2.   Tap **ok** to exit settings.

Band

> ![NOTE] **NOTE**   The **Band** tab appears only when MC75 configuration is installed on the mobile computer. Any changes made in this window do NOT persist after a cold boot (default settings are restored). Changes do persist after a warm boot.

1.   Tap **Start** > **Settings** > **Personal** tab > **Phone** icon > **Band** tab.

   or

   Start > **Phone** > **Menu** > **Options** > **Band** tab.
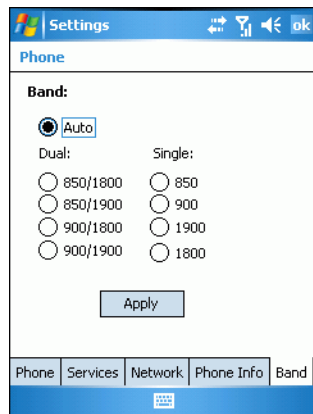
Figure 5-27   *Phone Window - Band Tab*

2.   Select the band that is associated with your network provider or select the **Auto** radio button to allow the mobile computer to automatically select the band.

3.   Tap **ok** to exit settings.

Chapter 6 MC9097 Configuration

Introduction

This chapter explains how to verify MC9097 service on an Integrated Digital Enhanced Network (iDEN) wireless network and establish settings.

iDEN is a wireless technology combining the capabilities of a digital cellular telephone, two-way radio, alphanumeric pager, and data/fax modem in a single network. iDEN operates in the 800 MHz, 900MHz bands and is based on time division multiple access (TDMA) and GSM architecture.

When using the MC9097 as a phone, services can include cellular voice, push-to-talk, speed dialing, voice mail, call forwarding and caller ID, depending on the type of service. The MC9097 is a Global Positioning System (GPS) capable device.

> **NOTE** Before a mobile computer can be used on an iDEN network, a voice and data-enabled service plan must be established and the mobile computer must be properly configured (where applicable).
>
> Refer to the *MC909X User Guide* for information on how to use the phone and services.

MC9097 Sprint Service Verification

MC9097 phone and data services require a SIM card, which is factory installed in the mobile computer. The SIM card has embedded circuitry on one side of its surface which provides phone service on an iDEN network. The SIM card provides a phone number, determines the features or services available to the subscriber and identifies the subscriber to the network.

Various settings may be required for the mobile computer to operate as a phone with data connection features.

Ensuring Network Coverage

1. Ensure an activated SIM card is installed in the mobile computer.

    > **NOTE** The SIM card must be iDEN enabled to connect to a network.

2. Tap **Start** > **Settings** > **Phone** icon > **Network** tab.
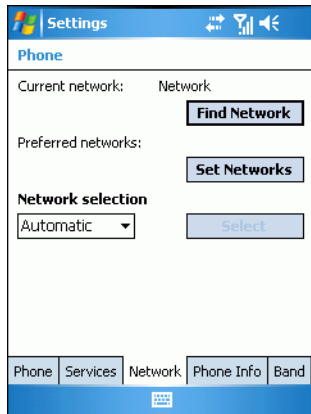
Figure 6-1   *Phone Settings Window - Network Tab*

3.   Ensure the service provider's network appears in the **Current network:** field.

4.   If the network does not appear, tap **Find Network**. If the network still does not appear, verify that the SIM card was installed correctly. If it was, and no network appears, contact the service provider.

Configuring an iDEN Data Connection

The MC9097 is pre-configured for data communication.

✓   *NOTE*   To verify active Nextel phone and data services, tap ⊞ to display the **Connectivity** dialog.

To set up a new data connection:

1.   Tap **Start** > **Settings** > **Connections** tab > **Connections** icon > **Tasks** tab.
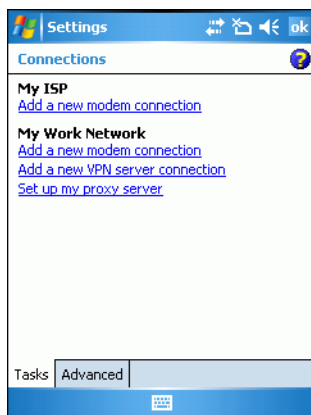
Figure 6-2   *Connections Window*

2.   Under **My ISP** select **Add a new modem connection**. The **Make New Connection** window appears.
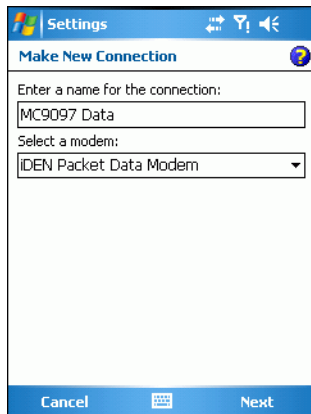
Figure 6-3   *Connections Window - Make New Connection*

3. Enter a connection name in the **Enter a name for the connection:** text box.

4. Select **iDEN Packet Data Modem** from the **Select a modem:** drop-down list.

5. Tap **Next**.
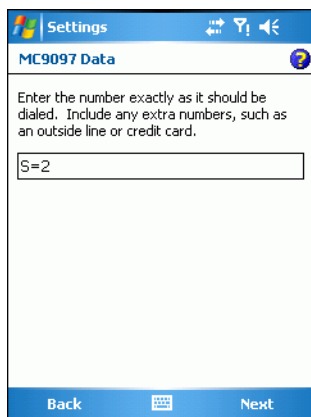
Figure 6-4   *Connections Window - Access Point Name*

6. Enter `s=2`.

7. Tap **Next**.
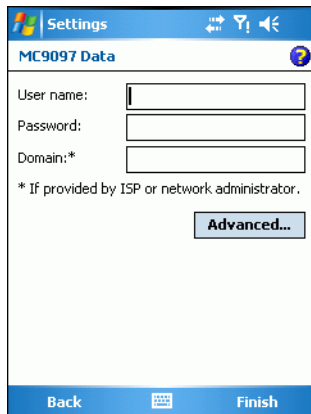
Figure 6-5   *Connections Window - User Name & Password*

8.   Tap **Finish** (user name and password are not required).

9.   Tap **ok** to exit **Connections**.

Establishing an iDEN Data Connection

1.   Ensure a SIM card is installed in the mobile computer.

2.   Ensure an iDEN data connection was configured. See *Configuring an iDEN Data Connection on page 6-2*.

3.   Tap   to display the **Connectivity** dialog box.
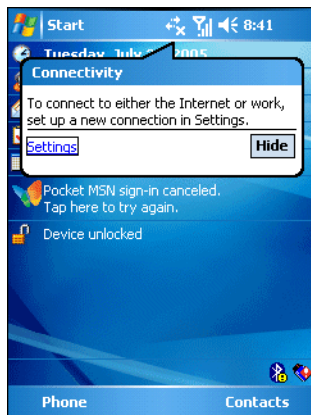
Figure 6-6   *Connectivity Dialog Box*

4.   Tap **Settings**.

5.   Tap **Managing existing connections**.

6.   Tap and hold on the data connection until a menu appears.
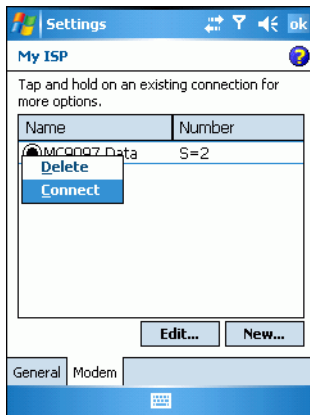
Figure 6-7 *Data Connection*

7.   Select **Connect**.

Figure 6-8 *Connecting Using IDEN Packet Data Modem*

8.   If the SIM card is protected with a Personal Identification Number (PIN), a dialog box pops up requesting the appropriate PIN to unlock the SIM card. In this case, enter the PIN and tap **ok**.

> *NOTE*   Emergency calls can be placed at any time without a SIM card installed or with an active SIM. If the SIM card is installed but inactive, emergency calls cannot be made. Remove the SIM card to make an emergency call. A PIN is not required to make an emergency call.

9.   When a connection is established, launch **Internet Explorer** to browse the Internet or launch an applicable application.

Ending an Data Connection

To end an established data connection:

1.   Tap to display the **Connectivity** dialog window.
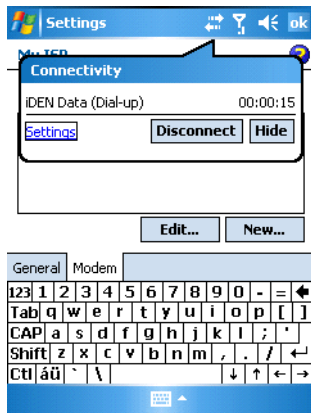
Figure 6-9   *Disconnecting a Data Connection*

2.   Tap **Disconnect**.

> ✓   *NOTE*   When **Disconnect** is tapped during an active data transfer (e.g., downloading a web page), the data connection automatically reconnects. The data connection cannot be disconnected until the data transfer is complete or terminated.

Phone Settings

Use the **Phone Settings** window to customize settings, such as the ring type and ring tone for incoming calls, security options and other options depending on the type of service.

Phone

Use the **Phone** tab to customize ring type, ring tone, keypad tone and security options.

Tap **Start** > **Settings** > **Personal** tab > **Phone** icon > **Phone** tab.

or

Start > **Phone** > **Menu** > **Options** > **Phone** tab.
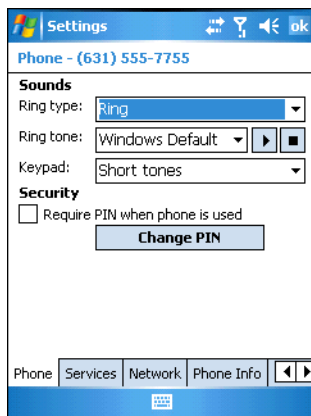
Figure 6-10   *MC9097 Phone Window - Phone Tab*

Sounds

> **NOTE**   After the first call is received, the Phone Number automatically displays on the **Phone** tab.

1. Select a ring type from the **Ring type:** drop-down list. The ring type changes the way the mobile computer rings to notify the user of an incoming call. Regardless of the ring type selected, a dialog box appears on the mobile computer's display for incoming calls.

2. Select a ring tone for incoming calls from the **Ring tone:** drop-down list. To hear a sample of the selected ring tone, tap ▶ . Tap ■ to end the ring tone.

> **NOTE**   To use custom .wav, .mid or .wma files as ring tones, use ActiveSync on the host computer to copy the file to the /Windows/Rings folder on the mobile computer. Then, select the sound from the ring tone list.

3. Select a keypad tone from the **Keypad:** drop-down list. This selection determines the tone that sounds when entering a phone number on the keypad.

    a. Select **Long Tones** for a continuous sound for as long as the number on the keypad is pressed.

    b. Select **Short Tones** for a tone that sounds only for one or two seconds.

    c. Select **Off** to disable tones.

Security

Enabling a PIN

| NOTE | Emergency calls can be placed at any time without a SIM card installed or with an active SIM. If the SIM card is installed but inactive, emergency calls cannot be made. Remove the SIM card to make an emergency call. A PIN is not required to make an emergency call. |

To require a PIN when using the phone:

1. Select the **Require PIN when phone is used** check box under **Security**.
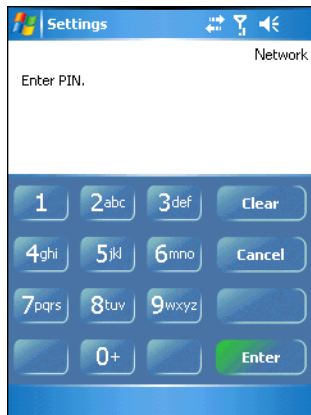
Figure 6-11   *Enter PIN*

2. Use the touch keypad to enter a four to eight digit PIN.

3. Tap **Enter** to enable the PIN and return to the **Phone** tab.

Changing a PIN

1. Tap **Change PIN**.
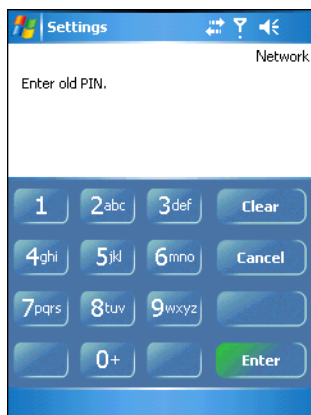
Figure 6-12   *Enter Old PIN*

2. Use the touch keypad to enter the current PIN.
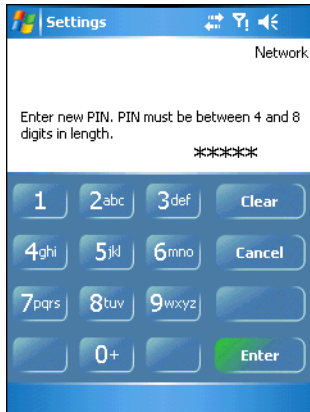
3. Tap **Enter**.

Figure 6-13   *Enter New PIN*

4. Use the touch keypad to enter a new four to eight digit PIN.

5. Tap **Enter**.

6. Reenter the new PIN for confirmation and tap **Enter**.

7. Tap **ok** to confirm the change.

Disabling a PIN

1. From the **Phone** tab, deselect the **Require PIN when phone is used** check box.

2. Use the touch keypad to enter the current PIN.

3. Tap **Enter**.

4. Tap **ok** to confirm the change.

5. Tap **ok** to exit settings.

Services

Use the **Services** tab to configure settings for subscribed phone services. For example, allow the caller's identity to be disclosed when making outgoing calls (*Caller ID on page 6-10*), forward incoming calls to a different phone number (*Call Forwarding on page 6-10*), be notified of incoming calls when a phone session is in use (*Call Waiting on page 6-11*) and set up voice mail and short message service (*Voice Mail and Text Messages on page 6-11*).

1. Tap **Start** > **Settings** > **Personal** tab > **Phone** icon > **Services** tab.

    or

    Start > **Phone** > **Menu** > **Options** > **Services** tab.
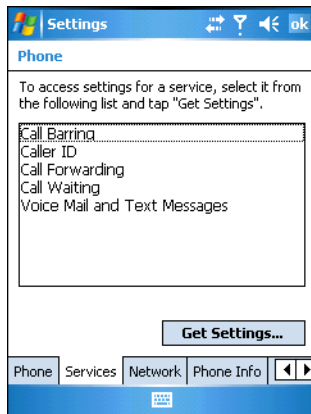
Figure 6-14   *MC9097 Phone Window - Services Tab*

2.   Select a service from the list and tap **Get Settings...** .

3.   Change services settings as follows.

Call Barring (Call Blocking)

Device initiated Call Barring is not supported. Please contact Sprint customer care to activate this service.

Caller ID

Enable caller ID to provide a way for people to know the identity of the person making an outgoing call. Select the **Everyone** radio button to always display the caller ID. Select the **No one** radio button to prevent the caller's identity from displaying to others.
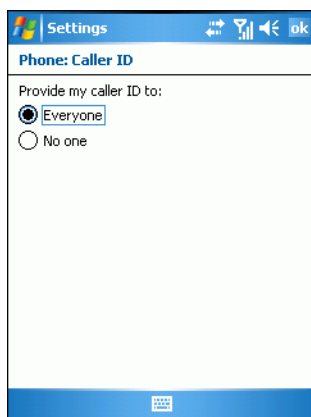
Figure 6-15   *Caller ID*

Call Forwarding

Use call forwarding to forward incoming calls to a different phone number.

- To forward all calls to a different phone number:
    - select the **Forward all incoming phone calls** check box.
    - enter the phone number to receive forwarded calls in the *To:* text box.

- To forward incoming calls to a different phone number based on a specific situation, select one or more of the check boxes under **Forward phone calls only if**:
  - **Unavailable:** enter the phone number to receive forwarded calls only when the phone is turned off or the user is unreachable.
  - **Busy:** enter the phone number to receive forwarded calls only when the line is busy.
  - **No answer:** enter the phone number to receive forwarded calls only when the phone cannot be answered.

Figure 6-16   *Call Forwarding*

Call Waiting

Call waiting notifies the user of an incoming call when the phone is in a phone session. Select the **Notify me** radio button to enable call waiting. Select the **Do not notify me** radio button to disable call waiting.
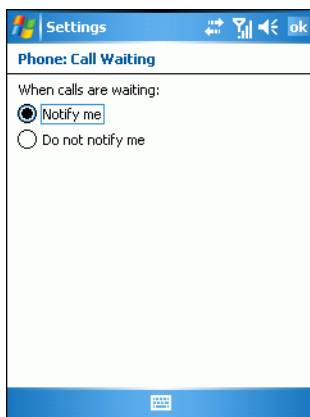
Figure 6-17   *Call Waiting*

Voice Mail and Text Messages

To retrieve voice mail, enter the your own phone number in the appropriate text box. (Short Message Service) SMS messages cannot be sent from the mobile computer but they are automatically received by the mobile computer.
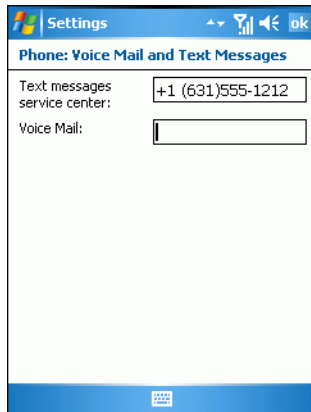
Figure 6-18   *Voice Mail and Text Messages*

Network

The **Network** tab indicates if the mobile computer is connected to the Nextel network.

Phone Info

NOTE   This property page is for diagnostics only and is not visible by default. To display this property page, navigate to the *Windows* directory using *File Explorer* and launch the *PropertyPages.exe* file. Follow the on-screen instructions for installation. To remove the property page clean boot the device.

Use the **Phone Info** tab to view specific phone information. The walkie-talkie phone number is the first item listed.

1. Tap **Start** > **Settings** > **Personal** tab > **Phone** icon > **Phone Info** tab.

   or

   Start > **Phone** > **Tools** > **Options** > **Phone Info** tab.
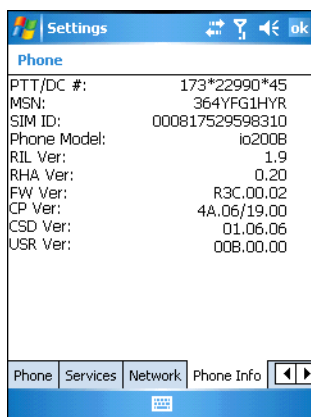
Figure 6-19   *MC9097 Phone Window - Phone Info Tab*

Table 6-1 *Phone Info Tab Data*

Item	Description
PPT/DC #	Lists the walkie-talkie phone number assigned to the SIM card installed in the mobile computer.
MSN	10 digit serial number of the io200 modem.
SIM ID	Lists the 15 digit SIM ID. THis number is also printed on the SIM card.
Phone Model	Lists the model number of the Motorola iDEN modem (io200B).
RIL Ver	Lists the Radio Interface Layer (RIL) version.
RHA Ver	Lists the Radio Hardware Abstraction (RHA) layer version.
FW Ver	Lists the Motorola radio firmware version.
CP Ver	Code Plug settings version. This defines the default modem and phone characteristics. This can be written to remember any change to the default settings.
USR Ver	User Data File that defines carrier specific default values for the modem.

2. Tap **ok** to exit.

GPS

NOTE This property page is for diagnostics only and is not visible by default. To display this property page, navigate to the *Windows* directory using *File Explorer* and launch the *PropertyPages.exe* file. Follow the on-screen instructions for installation. To remove the property page clean boot the device.

Use the **GPS** tab for GPS diagnostics. The GPS tab is not a functional applications.

1. Tap **Start** > **Settings** > **Personal** tab > **Phone** icon > **GPS** tab.

    or

    Start > **Phone** > **Tools** > **Options** > **Phone Info** tab.
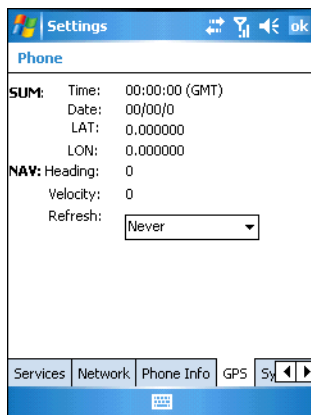
Figure 6-20 *MC9097 Phone Window - GPS Tab*

2. In the **Refresh** drop-down list, select a refresh time frame.

NOTE Setting the **Refresh** value enables the GPS radio and can drain the battery if left on.

3. Tap **ok** to exit settings.

Sys Stat

> ✓ *NOTE*   This property page is for diagnostics only and is not visible by default. To display this property page, navigate to the *Windows* directory using *File Explorer* and launch the *PropertyPages.exe* file. Follow the on-screen instructions for installation. To remove the property page clean boot the device.

Use the **Sys Stat** tab to view system information.

1. Tap **Start** > **Settings** > **Personal** tab > **Phone** icon > **Sys Stat** tab.

    or

    Start > **Phone** > **Tools** > **Options** > **Phone Info** tab.
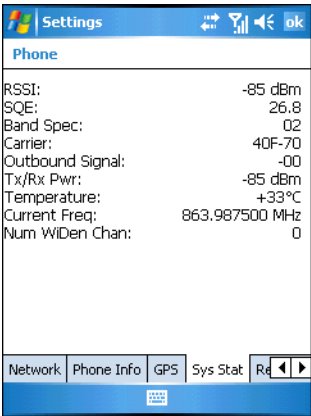
Figure 6-21   *MC9097 Phone Window - Sys Stat Tab*

Table 6-2   *Sys Stat Tab Data*

Item	Description
RSSI	Lists the Received Signal Strength Indicator in dBm. Usually between -104 and -80. -80 is a very strong signal and -104 is very weak.
SQE	Lists the Signal Quality estimate. Gives a measure of signal quality where RSSI gives a measure of signal strength. Values around 20 are good.
Band Spec	Lists the Band Specifier that restricts the modem to a certain band of frequencies.
Carrier	Lists the current frequency that the modem is tuned into and is interpreted as: XXX-YZ where XXX is the carrier number, Y is the color code and Z is the extended color code.
Outbound Signal	Lists the signal quality of the received RF signal.
Tx/Rx Pwr	Duplicate of RSSI field.

Table 6-2 *Sys Stat Tab Data*

Item	Description
Temperature	Lists the temperature, in degrees C, of the Motorola iDEN modem.
Current Freq	Lists the receive frequency in MHz of the Motorola iDEN modem. There are just under 2000 different transmit frequencies supported. This is selected by modem - carrier negotiations.
Num WiDEN Chan	Lists the number of WiDEN channels being used to transmit.

2. Tap **ok** to exit settings.

Reg Stat

> **NOTE** This property page is for diagnostics only and is not visible by default. To display this property page, navigate to the *Windows* directory using *File Explorer* and launch the *PropertyPages.exe* file. Follow the on-screen instructions for installation. To remove the property page clean boot the device.

Use the **Reg Stat** tab to view registration information.

1. Tap **Start** > **Settings** > **Personal** tab > **Phone** icon > **Reg Stat** tab.

or

Start > **Phone** > **Tools** > **Options** > **Reg Stat** tab.

Figure 6-22 *MC9097 Phone Window - Reg Stat Tab*

Table 6-3 *Reg Stat Tab Data*

Item	Description
Dispatch	Lists the registration status of the specified service. Displayed as <service> <status> <code> where: <service> = NS - No Service; IS - In Service; <status> = 0 - No Info; 1 - Accept; 2 - Reject; <code> = A numeric value
Interconnect	Same as above item.
Packet Data	Same as above except <status> can have the value 3 - Accept WiDEN

Table 6-3   *Reg Stat Tab Data*

Item	Description
Mobile IP	Same as above item.
Phone Restricted	Same as above item.
NEI - IP	Lists the IP address assigned to this modem. This address is required for packet data.
Home Agent	Lists the Mobile IP Home Agent that the user is registered with.
DNS - Pri	Lists the IP address of the Primary Domain Name Server.
DNS - Sec	Lists the IP address of the Secondary Domain Name Server.

2.   Tap **ok** to exit settings.

Error Log

> *NOTE*   This property page is for diagnostics only and is not visible by default. To display this property page, navigate to the *Windows* directory using *File Explorer* and launch the *PropertyPages.exe* file. Follow the on-screen instructions for installation. To remove the property page clean boot the device.

The **Error Log** tab provides diagnostic information and tools.

Tap **Start** > **Settings** > **Personal** tab > **Phone** icon > **Error Log** tab.

or

Start > **Phone** > **Tools** > **Options** > **Error Log** tab.
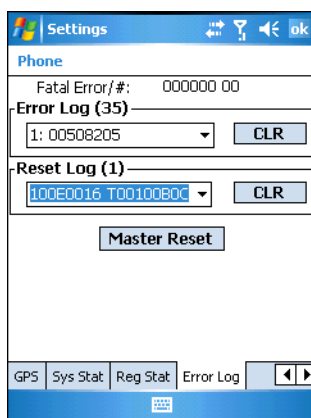
Figure 6-23   *MC9097 Phone Window - Error LogTab*

Tap **ok** to exit settings.

The **Master Reset** button resets the iDEN radio inside the mobile computer.

Chapter 7 Application Deployment for WinCE 5.0

Software Installation on Development PC

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

- Symbol Mobility Developer Kit (SMDK) for C
- Windows CE Platform SDK for MC9090
- Device Configuration Package (DCP) for MC9090.

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

The Windows CE Platform SDK for the MC909X is used in conjunction with the SMDK for C to create Windows CE applications for the MC909X mobile computer. The Platform SDK installs a new Windows CE device type and its associated libraries onto the development PC. This new device is added to the Active WCE Configuration field of Microsoft eMbedded Visual C++ 4.0.

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

DCP for MC9090

To install the DCP for MC9090:

1. Download the DCP from the Support Central website, http://support.symbol.com:
   a. On http://support.symbol.com, select **Software Downloads**.
   b. Select **Mobile Computers**.
   c. Select **MC9090 CE**.
   d. Select *Device Configuration Package (DCP) for MC9090*.
   e. Save the .exe file to the development computer.

2. Locate the .exe file on the development computer, double-click the file, and follow the install screen prompts.

3. Once installed, access the major components of the DCP from the *Symbol Device Configuration Package (DCP) for MC9090* program group of the *Windows Start Menu.*

Platform SDK

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

1. Download the appropriate Platform SDK from the Support Central web site, http://support.symbol.com.

   a. On http://support.symbol.com, select **Software Downloads**.

   b. Select **Mobile Computers**.

   c. Select **MC9090 CE**.

   d. Select Platform for the MC909X.

   e. Save the .exe file to the development computer.

2. Run the file and follow the screen prompts to install.

Symbol Mobility Developer Kits

To install an SMDK:

1. Download the SMDK from the Support Central website, http://support.symbol.com:

   a. On http://support.symbol.com, select **Software Downloads**.

   b. Select **Mobile Computers**.

   c. Select **MC9090 CE**.

   d. Select *Symbol Mobility Developer Kit.*

   e. Select the latest version, then download the .exe file to the development computer.

2. Double-click the executable file and follow the install screen prompts.

Installing Other Development Software

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

Deployment

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

Download/Install software using:

- ActiveSync

- SD Card

- IPL.

ActiveSync

Use ActiveSync to copy files from a host computer to the mobile computer.

1.   Ensure that ActiveSync is installed and that a partnership has been created, see *Chapter 3, ActiveSync*.

2.   Connect the mobile computer to the host computer using a USB cradle or an appropriate cable, see *Chapter 2, Accessories* for connection information.

3.   On the host computer, select **Start** > **Programs** > **ActiveSync**.

4.   Select **Explore**.
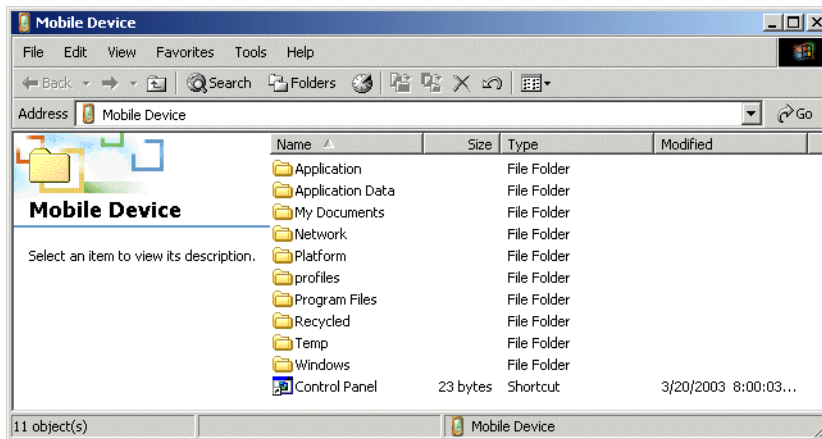
Figure 7-1   *ActiveSync Explorer*

5.   Double-click the folder to expand the contents of the folder.
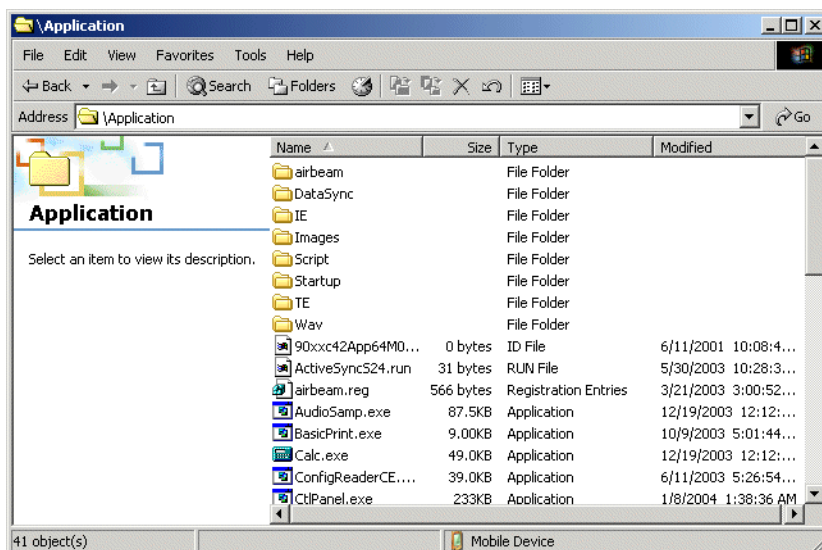
Figure 7-2   *My Pocket PC Contents*

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.

SD Card

The SD card can be used to download/upload files to and from the mobile computer. See *Multi Media Card (MMC) / Secure Device (SD) Card on page 2-4* for instruction on installing an SD card. To view the contents of the SD Card, open **Windows Explorer** and select **Storage Card**. You can copy files from the SD Card to the mobile computer or double-tap the executable file to launch the application.

IPL

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

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

There are two types of update 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:

- 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 Using IPL on page 7-11* for procedures on downloading a hex file to the mobile computer.

Creating 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 for MC9090c50 includes scripts used by Symbol Technologies 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 Device Configuration Packages\MC9090x\v1.0\TCM Scripts.*

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

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

- Starting TCM
- Defining script properties
- Creating the script for the hex image
- Building the image
- Sending the hex image
- Creating a splash screen
- Flash storage.

Starting Terminal Configuration Manager

Click the Windows start menu TCM icon (*Symbol Device Configuration Packages*, *MC9090c50*) to start TCM. The **TCM** window appears displaying two child windows: **Script1** and **File Explorer**. The **Script1** window contains a newly created script and the **File Explorer** window contains a file explorer view used for selecting files to be placed in the script.
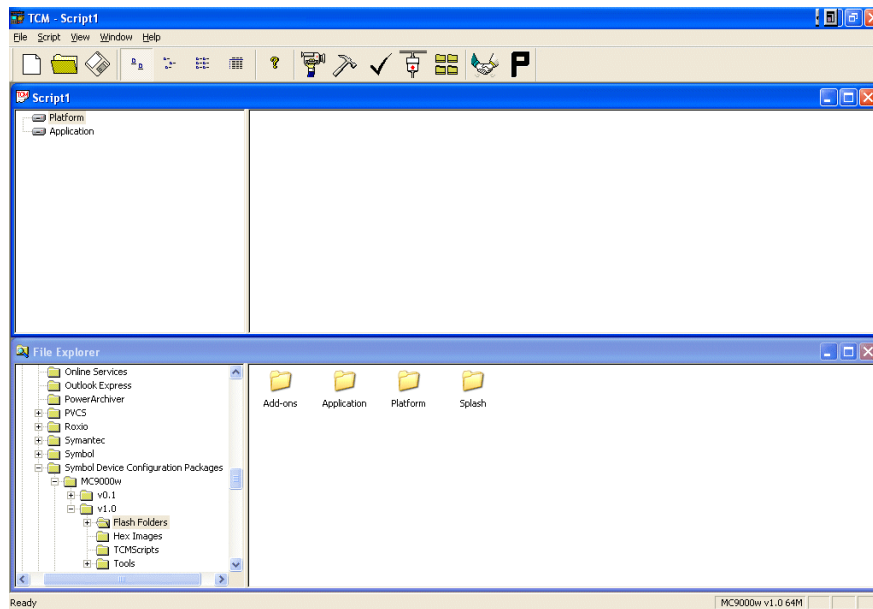
Figure 7-3   *TCM Startup Window*

The following table lists the components of the TCM window.

Table 7-1   *TCM Components*

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

Table 7-1   *TCM Components (Continued)*

Icon	Component	Function
	Large icons button	View the current script items as large icon.
	Small icons button	View the current script items as small icon.
	List button	View the current script items as a list.
	Details button	View the current script items with more details.
	About button	Display version information for TCM.
	Properties button	View/change the current script properties.
	Build button	Build the current script into a set of hex files.
	Check button	Check the script for errors (files not found).
	Send button	Download the hex image to the mobile computer.

Table 7-1   *TCM Components (Continued)*

Icon	Component	Function
	Tile button	Arrange the sub-windows in a tiled orientation.
	Build and Send	Build the current script into a set of hex images and send the hex images to the mobile computer.
	Preferences button	View/change the global TCM options.

Defining Script Properties

Before a script is created, the script properties must be defined. This defines the type of 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.
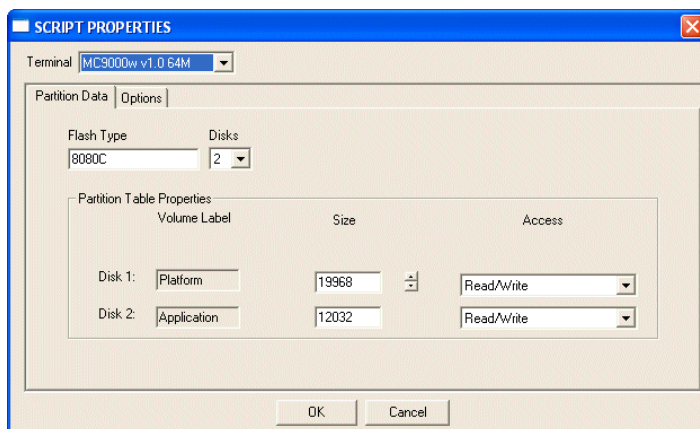
Figure 7-4   *Script Properties Window - Partition Data Tab*

3. In the **Terminal** drop-down list, select the terminal type.

4. Use the default **Flash Type**.

5. In the **Disks** drop-down list, select the number of disk partitions to create.

6. Select the (memory) **Size** for each partition. Note that adding space to one disk. partition subtracts it from another.

7. In the **Access** drop-down list for each disk partition, determine and select the Read/Write access option.

8. Click the **Options** tab. The **Script Properties** *window* > **Options** tab appears.
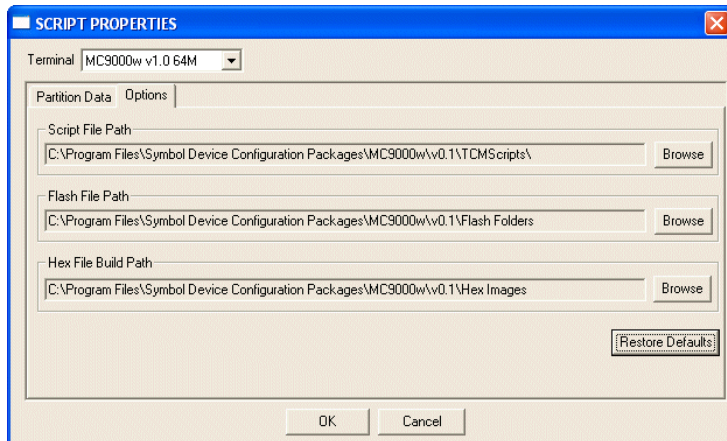
Figure 7-5 *Script Properties Window - Options Tab*

9. Set the paths for the Script File, Flash File and Hex File Build.

10. Click **OK**.

Creating the Script for the Hex Image

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

\Program Files\Symbol Device Configuration Packages\MC9000w\v0.1\TCMScripts\

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

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

Opening a New or Existing Script

A script file can be created from scratch or based on an existing script file. Click **Create** to create a new script or click **Open** to open an existing script (for example, a script provided in the DCP for MC9000w). If an existing script is opened and changes are made, saving the changes overwrites the original script. To use an original or Symbol supplied standard script as a base and save the changes in a new script, use the *Save As* function to save the script using a different file name.

Updating TCM 1.X Scripts

Script files that were created with older versions of TCM can be upgraded to TCM 2.0 scripts. Click **Open** to open an existing script created with an older version of TCM. The *Conversion* window appears automatically.
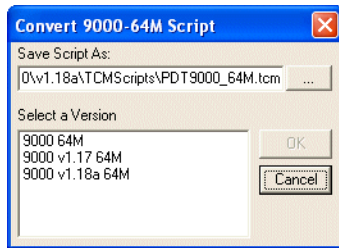
Figure 7-6   *Conversion Window - Upgrading to TCM 2.0*

Copying Components to the Script

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

Saving the Script

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

Building the Image

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

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

To build scripts:

1. Click **Build** on the TCM toolbar. The **Configure Build** window appears.
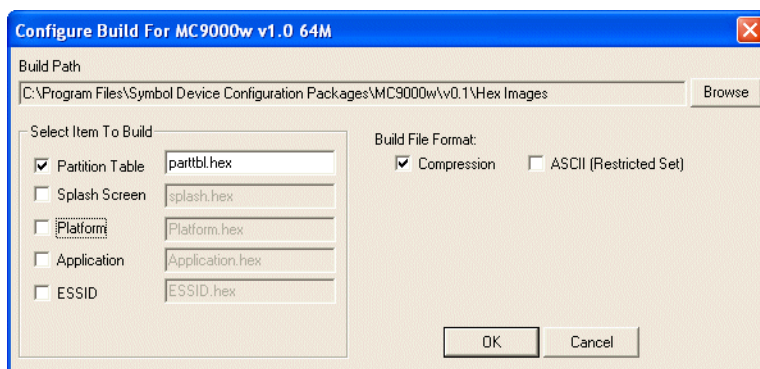
Figure 7-7   *Configure Build Window*

2. Select the items (partitions) to build using the check box(es) to the left of each named partition.

3. The **Build Path** defines where to store all built partitions.

4. Select (hex image) COMPRESSION to reduce the size and speed up the download.

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

   If one of the partitions being built is the ESSID, a prompt appears requesting the ESSID value. Deselect the HR (High Rate) check box when building ESSID images for a device with an FH radio.
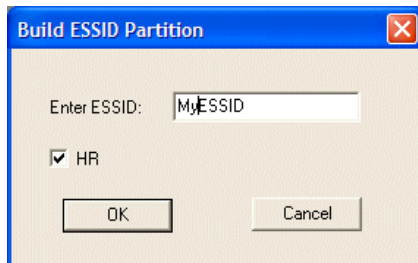
Figure 7-8   *Build ESSID Partition Window*

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

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

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

- Files defined in the script can not be found. This error can occur when the files referenced by the script are no longer stored on the development computer or the folders where they are stored were renamed.

- The total amount of flash memory space required by the script exceeds the image size. To correct this, reduce the number of files in the partition or increase the size of the partition. See *Defining Script Properties on page 7-8* for more information about setting the image size appropriately.

Sending the Hex Image Using IPL

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

> *NOTE* If you are using an SD/MMC memory card to load a hex image onto the mobile computer, you must first copy the files to the SD/MMC card and install the card into the memory slot under the keyboard. See *Multi Media Card (MMC) / Secure Device (SD) Card on page 2-4* for instructions for installing an SD/MMC card.

1. Press the battery eject button to release the battery but do not remove completely.

2. Press and hold the trigger and the **Power** button while re-inserting the battery until the mobile computer resets into IPL.

3. Release the power button while holding down the trigger.

4. Insert the mobile computer into cradle or connect CAM while continuing to hold the trigger.

> *NOTE* The mobile computer must be inserted in the cradle or attached to the CAM, both with their appropriate power supplies connected to a power source, for the mobile computer to reset into IPL.

5. Release the trigger. The **Initial Program Loader** menu appears.

```
Initial Program Loader


Platform
Application
Windows CE
Monitor
Splash Screen
Power Micro
Partition Table
Command File
System Reset
Auto Select
```
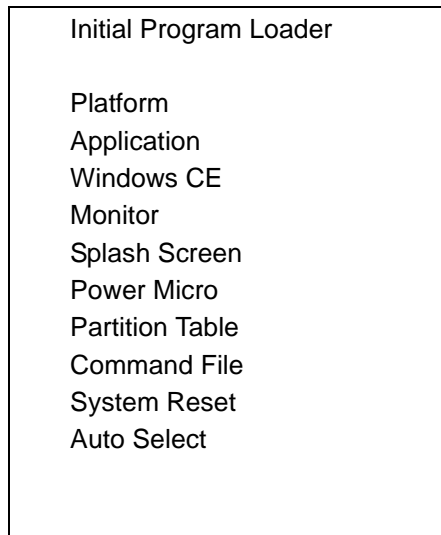
Figure 7-9   *Initial Program Loader (IPL) Menu*

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

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

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

Table 7-2   *IPL Menu Partitions*

Partition Name	Description
Platform	Contains the files in the *Platform* folder.
Application	Contains the files in the *Application* folder.
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. Note: Splash screens are generated from .bmp images and must be less than or equal to 240 pixels wide and 296 pixels deep. For mono displays, the bmp image must be 4 bpp and for color screens the color depth must be 8 bpp. Note: 8 bits per pixel only applies to splash screen images. Once Windows CE is running, the color density is 16 bits per pixel.
Power Micro	The Power Micro is a small computer contained within the 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.

Table 7-2   *IPL Menu Partitions (Continued)*

Partition Name	Description
Partition Table	Contains the partition information for all other partitions.
	Note: The partition table should never need changing unless the sizes of the platform and application images are changed within TCM. If this is done, then the new partition table should be loaded first, followed by both platform and application in any order.
Command File	Select to load a command file. A command file is a file that allows you to automatically load a number of partitions in a batch process.
System Reset	Selecting this item provides a simple method to exit IPL and to boot the operating system.
Auto Select	Selecting this item allows one or more files to be downloaded without having to manually select the destination. (The content of the files being downloaded automatically directs the file to the correct destination.) For technical reasons, Auto Select cannot be used to download Monitor, Power Micro, or Partition Table. These items must be specifically selected.

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

```
Select Transport

USB
SD/MMC
Lighthouse 0 - Serial
Previous
Top
```
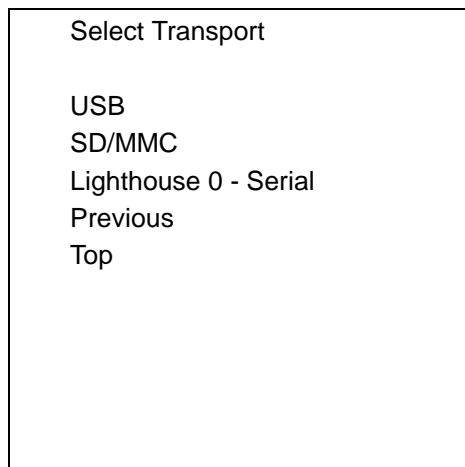
Figure 7-10   *Select Transport Menu*

8.   Use the up and down scroll buttons to select the method of transport, then press **Enter**.

9.   If you selected the **Lighthouse 0 - Serial** transport method:

    a.   the **Baud Rate Menu** appears.

```
Baud Rate Menu
115200
57600
38400
19200
9600
Previous
Top



```
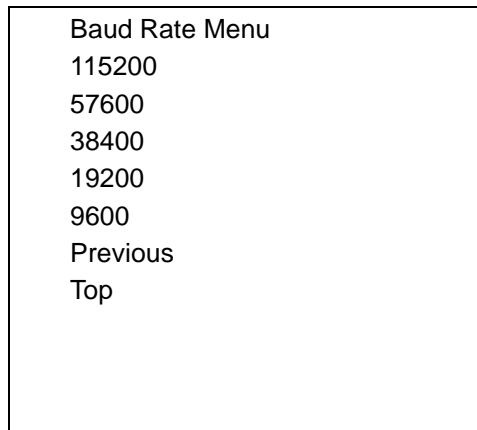
Figure 7-11 *Baud Rate Menu*

    b.   Use the up and down scroll buttons to select the appropriate baud rate, then press **Enter**.

10. If you selected **USB** transport method press **Enter**. If this is the first time using USB transport, you might need to install the Symbol USB driver. Follow the screen prompts.

11. If you selected **SD/MMC** transport method:

    a.   The mobile computer scans the memory card for files.

    b.   Select the file to download.

    c.   Press **Enter**.

12. The **Download File?** menu appears.

```
Download File?

Download
Cancel
Show Parms
Previous
Top



```
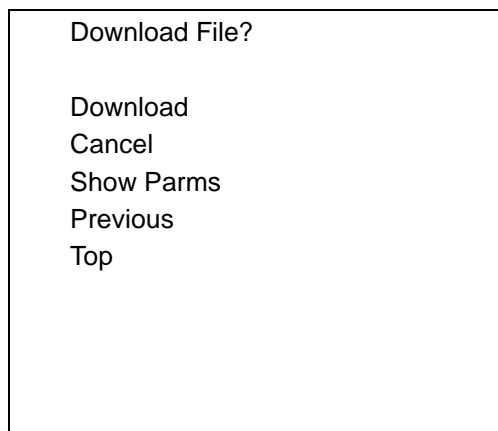
Figure 7-12 *Download File? Menu*

13. Use the up and down scroll buttons to select **Show Parms** to verify the file to download. Press **Enter** to display the **Parameters** screen.

```
Download:
"Partition Name" via
"Device Parameters"


Press Enter to Continue
```
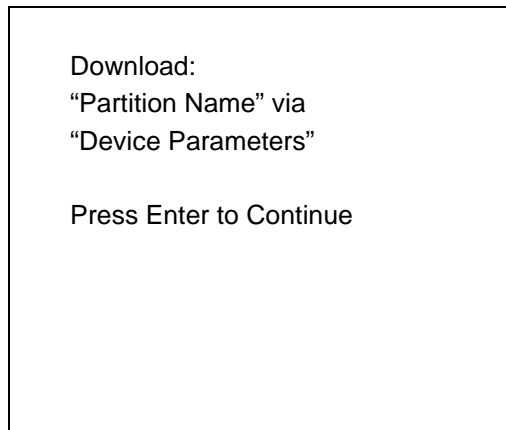
Figure 7-13   *Parameters Screen*

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

Device Parameters is the device selected in the **Select Transport** menu with the baud rate for serial downloads, or *DHCP address* for wireless downloads.

14. Press **Enter** to return to the **Download File?** menu.

15. Use the up and down scroll buttons to select **Download**. Press **Enter**. The **Downloading** screen appears.

```
Downloading:
Partition Name

Device Parameters

Device Status
```
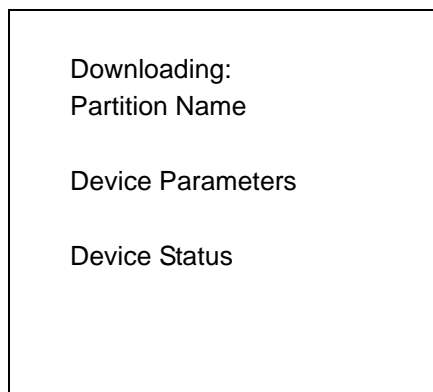
Figure 7-14   *Downloading Screen*

Before the download starts, if **Lighthouse 0 - Serial** or **USB** was selected in the **Select Transport** menu, **Waiting for Data** appears in the **Device Status** field.

16. On the development computer, click **Load** on the TCM toolbar. The **Load Terminal** window > **Serial** tab appears.
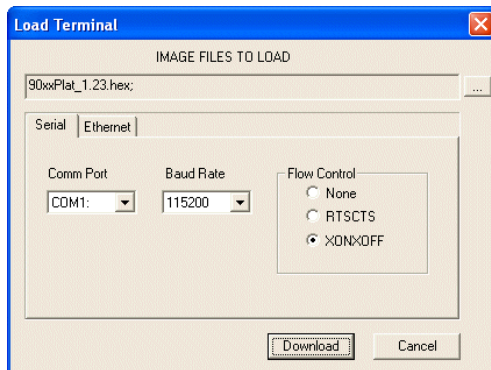
Figure 7-15　*Load Terminal Window - Serial and Ethernet Tabs*

17. Select the **Image Files To Load**, **Comm Port** and **Baud Rate** from their respective drop-down lists.

18. Click **Download** to begin the operation.

19. During download, the **Downloading** screen on mobile computer displays the **Device Status** and a progress bar.

20. When complete, **Device Status** displays **Result was Success**, or in the case of an error, the cause of the error.

21. On completion, press **Enter** to return to the IPL menu to select the next partition to download.

22. To exit IPL, select the **System Reset** item from the IPL menu (see *Figure 7-9 on page 7-12*).

TCM Error Messages

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

Table 7-3　*TCM Error Messages*

Error	Description/Solution
Failed to build images: flash file system DLL not loaded!	TCM could not load the DLL required to build images for the targeting flash file system. Reinstall TCM or recover the DLL.
Failure finding directory xxx	Building process failed because directory xxx was not found.
Failure creating volume	Building process failed because a certain disk volume could not be created.
Failure adding system file to image	Build process failed because TCM failed to add a certain system file to the disk image.
INVALID PATH	The path for the image file to build is not valid.
Nothing Selected To Build	In the Config Build window, no item is selected to build.
Illegal ESS ID	In the Build ESSID Partition window, no ESS ID was entered or the ESS ID entered was illegal.
Disk Full	TCM failed to create Hex image file at the selected path. Check available disk space.

Table 7-3 *TCM Error Messages (Continued)*

Error	Description/Solution
Target Disk Full	Build process failed because TCM failed to add file to the image of a disk volume. Remove some files or increase the disk size.
Hex file is READ ONLY	The Hex image file to be created exists and is read-only. Delete the existing file or change its attribute.
Error opening the file xxx with write access	TCM could not open file xxx with write access. Check if file is in use.
Failure creating binary file	TCM failed to open/create an intermediate binary file.
Hex File To load is missing or invalid	In Load Terminal window, the file selected to load has invalid status.
Could not locate 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
```
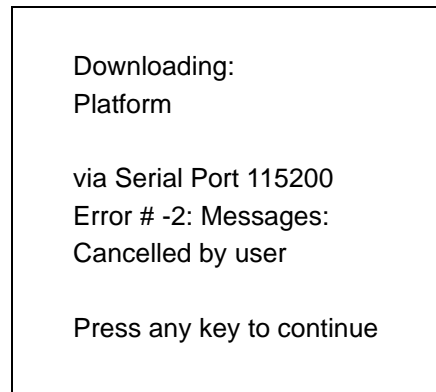
Figure 7-16   *IPL Error Screen*

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

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

Table 7-4   *IPL Errors*

Error Text	Error Number	Probable Cause
Unknown error	-1	A general error occurred. Retry the download. If the failure persists, it is most likely due to a hardware failure; the mobile computer requires servicing.
Cancelled by user	-2	The user canceled the download.
Can't open the source	-7	An error occurred opening the source device (either radio card or Serial port). Check source device connectivity and retry.
Can't open the destination	-8	An error occurred opening the destination device (either flash ROM or Power Micro). Retry the download. If the failure persists, it is most likely due to a hardware failure; the 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 7-4   *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 Main Menu (not Auto Select) but the file selected for download was for another partition. Ensure that the partition selected from the Main Menu matches the file selected for download.
File type does not support IPL Auto Select	-29	Monitor, Power Micro and Partition Table cannot be loaded with Auto Select. Select the appropriate area, and try again.
Non-contiguous record found	-30	A Symbol HEX file download was attempted but the HEX file is invalid. Ensure the file is in Symbol HEX file format.
Timed Out - No data	-31	IPL was waiting for data from the source device but timed out before receiving any. Check the source device connectivity and retry.
Fail: Buffer Overrun	-32	The serial port device could not keep up with incoming data. Retry the serial download with a lower baud rate.
Partition Table not Valid	-33	The size of flash memory is different than that described in the partition table. Retry the download with the correct partition table file.
Invalid file format	-34	The file format is invalid. Only Symbol HEX files are supported by IPL.

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 MC9090c50. 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 MC9090c50 using an image editor.

2. For mobile computers with color screens, open the Splashcolor.bmp file supplied with the DCP for MC9090c50 using an image editor.

3. Modify the bitmap file and save.

4. Create a splash partition using the steps shown in the *Building the Image on page 7-10*.

Splash Screen Format

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

Table 7-5   *Splash Screen Format*

Screen Type	Dimensions	Color Format
Monochrome	240x296	4 bits per pixel
Color	240x296	8 bits per pixel*
* 8 bits per pixel only applies to splash screen images. Once Windows CE is running, the color density is 16 bits per pixel.		

See *Sending the Hex Image Using IPL on page 7-11* for information about loading the splash screen using TCM and IPL.

Flash Storage

In addition to the RAM-based storage standard on Windows CE 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 Symbol-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 9000 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 MC9000w contains examples of .reg files.

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

Typically, do not make modifications to registry values for drivers loaded before RegMerge. However, these values may require modification during software development. Since these early loading drivers read these keys before RegMerge gets a chance to change them, the 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 MC9090c50. It can also be obtained from the Support Central web site at http://support.symbol.com/.

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 Symbol. The current OS partition on the mobile computer is included as part of the TCM installation package. Any upgrades must be obtained from Symbol. 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 7-19*.

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

- IPL: This program interfaces with the host computer and allows downloading via cradle or serial cable any or all of the partitions listed above, as well as updated versions of IPL. Use caution downloading updated IPL versions; incorrect downloading of an IPL causes permanent damage to the 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.

Chapter 8 Application Deployment for Mobile 5.0

Introduction

This chapter describes new features in Windows Mobile 5.0 including new security features, how to package applications, and procedures for deploying applications onto the mobile computer.

Security

The MC909X mobile computers 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 mobile computer.

- Trusted - All applications must be digitally signed by a certificate on the mobile computer.
- 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 Symbol's software certificate, they are assured that the package is authentic and that it was created by Symbol. By enforcing the use of digital signatures, users can also prevent malicious applications from executing on the mobile computer. For example, users can provision the mobile computer to only execute "trusted" applications (digitally signed).

Symbol ships all Windows Mobile 5.0 based products in an "open" state, which means all signed and unsigned applications should work. However, customers can still reconfigure their mobile computers 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 5.0 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 5.0, 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 5.0 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, Symbol ships with RAPI in the restricted mode. Certain tools, such as RAPIConfig, may

not work properly. Refer to the *Windows Mobile Version 5.0 Help* file for finding information on Remote API security policies.

Packaging

> ✓ **NOTE**   Applications compiled for Windows Mobile 5.0 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 mobile computer. Package new applications and updates, such as new DLL files, as CAB files, then deploy them to Windows Mobile 5.0 devices. Refer to the *Microsoft Windows Mobile 5.0 Help* file for information on CAB files.

Deployment

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

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

Refer to the *Microsoft Windows Mobile 5.0 Help* file for information on CAB files.

Installation Using ActiveSync

To install an application package:

- Connect the mobile computer 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 mobile computer.
- Copy the CAB file from the host computer to the \temp directory on the mobile computer.
- On the mobile computer, navigate to the \temp directory.
- Tap on the application CAB file. The application installs on the mobile computer.

Installation Using Storage Card

To install an application package:

- Copy the package CAB file to a storage card using an appropriate storage card reader.
- Install the storage card into the mobile computer. See *Multi Media Card (MMC) / Secure Device (SD) Card on page 2-4* for more information.

- On the mobile computer, open **File Explorer**.

- Open the **Storage Card** directory.

- Tap the package CAB file. The application installs on the mobile computer.

Installation Using AirBEAM

See *Chapter 9, Staging and Provisioning* for information on AirBEAM.

MSP 3.X

See *Chapter 9, Staging and Provisioning* for information on MSP 3.X.

Image Update

Windows Mobile 5.0 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. Symbol distributes the update packages on the Support Central web site, http://support.symbol.com.

To update an operating system component, copy the update package to the mobile computer using one of a variety of transports, including ActiveSync, an SD memory card, or Symbol AirBEAM. 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.

- Use AirBEAM.

> *NOTE*   The mobile computer 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://support.symbol.com.

2. Download the appropriate update package.

3. Copy the update package to either the \temp directory on the mobile computer, or to a storage card.

4. Connect the mobile computer to AC power. See *Chapter 2, Accessories*.

5. Press the primary battery release on the mobile computer to partially eject the battery from the mobile computer.

6. On an MC9090-G, while the battery is partially released, simultaneously press and release the trigger and the **Power** button.

   or

   On an MC909X-K or MC909X-S, while the battery is partially released, simultaneously press and release the left scan trigger and the **Power** button.

> *NOTE*   After you insert the battery you have 2 seconds to press the trigger or left scan button.

7.   Push the battery to fully re-insert it in the mobile computer. One audible click can be heard as the battery is fully inserted.

8.   On the MC9090-G, press and hold the trigger.

     or

     On the MC909X-K or MC909X-S, press and hold the left scan button.

9.   Connect the mobile computer to AC power using the CAM or insert the mobile computer into a powered cradle.

10. The Update Loader application first looks for a file on a storage card. If it does not find it, it looks in the \temp directory.

     When it finds the appropriate file, it loads the package onto the mobile computer. A progress bar displays until the update completes.

11. The mobile computer re-boots.

12. The calibration screen appears.

> **NOTE**   When initiating an update via a boot sequence, the update loader looks for updates first on the root of an installed SD card and then in the \temp folder on the mobile computer's persistent storage volume. A response file, pkgs.lst, indicates which files to update. In most cases, Symbol 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 mobile computer. 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: 240 x 296.

     •   Colors: 8 bits per pixel (256 colors) for color displays.

2.   Modify the bitmap file and save.

To load the splash screen on the mobile computer:

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:

     •   SD card root directory

     •   mobile computer's \temp directory

     •   mobile computer's \Windows directory.

3.   If using an SD card, insert the SD card into the mobile computer.

4.   Perform a cold boot.

5.   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 a mobile computer XML provisioning should be used. To install an XML provisioning file on the mobile computer, create a Cabinet Provisioning File (CPF) file. 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 mobile computer. The user receives an e-mail notification indicating success or failure.

XML Provisioning provides the ability to configure various features of the mobile computer (i.e., registry and file system). However, some settings require security privileges. To change registry settings via a CPF file, you need to 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 Windows Mobile 5.0 Help file, *Metabase Settings for Registry Configuration Service Provider* section, for the default role settings in Windows Mobile 5.0.

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 5.0 Help* file and the *Windows Mobile 5.0 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 below and rename it _setup.xml.) Ensure the file contains the required parameters for the operation. Refer to the *Microsoft Windows Mobile 5.0 Help* file for information.

2. In the Windows Mobile 5.0 tools directory on the desktop computer (typically \Program Files\Windows CE Tools\wce500\Windows Mobile 5.0 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 mobile computer. Refer to the *Windows Mobile Version 5.0 Help* file for more information.

XML Provisioning vs. RegMerge and CopyFiles

Prior to Windows Mobile 5.0, Symbol used two drivers (RegMerge and CopyFiles) to update the registry and to copy files during a cold boot. With Windows Mobile 5.0, Symbol recommends using XML provisioning instead. RegMerge and CopyFiles are supported for backward compatibility but Symbol 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="filesystem">
                <characteristic type="Copy">
                    <parm name="Source" value="\Application\example.txt" translation="filesystem"/>
                </characteristic>
            </characteristic>
        </characteristic>
    </characteristic>
</wap-provisioningdoc>
```

Storage

Windows Mobile 5.0 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 5.0 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, Symbol 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 mobile computer 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 5.0 protects all data and applications from power-related loss. Because Windows Mobile 5.0 mounts the entire file system and registry in persistent storage (rather than using RAM), MC909X 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).

Symbol Configuration Manager

Symbol Configuration Manager (SCM) is a utility that runs on the host computer and is used to create configuration files. These files, when deployed to an vehicle computer, set configuration parameters for that device. The configurable options for a vehicle computer are defined in an XML file that is available on the Support Central. 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:

- Symbol Configuration Template (.SCT) 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 mobile computer 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 8-1* shows the main window for a device's .sct file.
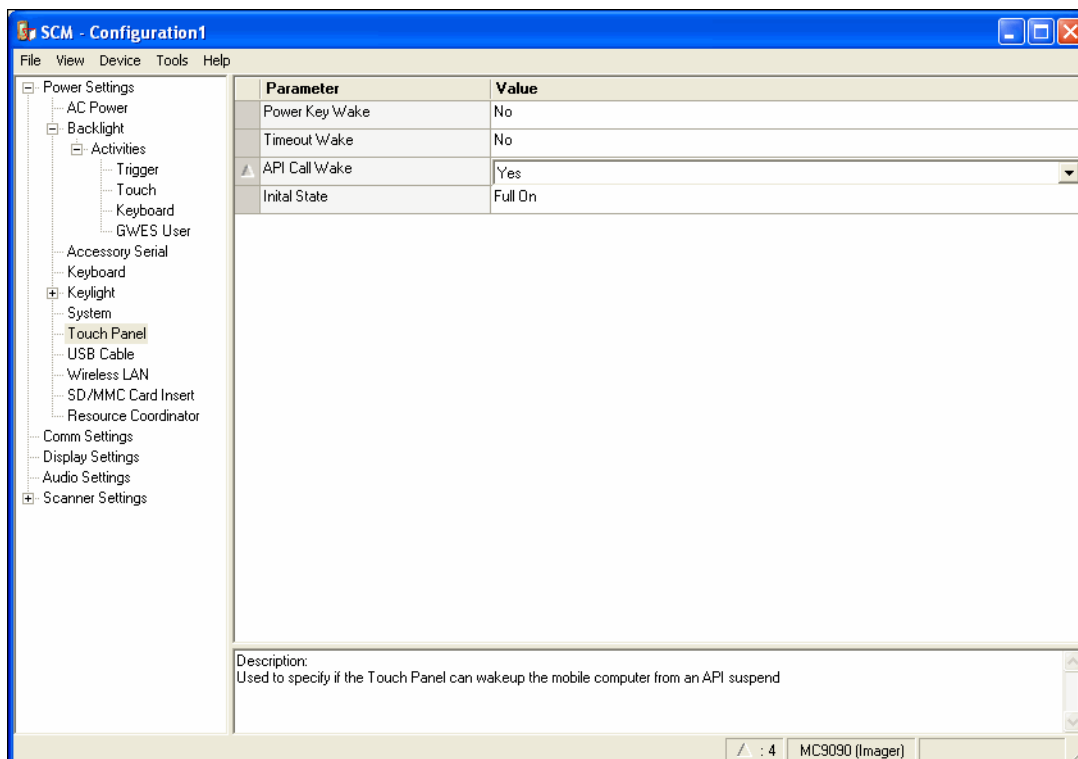
Figure 8-1   *Main SCM Window*

Menu Functions

Use the main menu to access the program functionality described in *Table 8-1*.

Table 8-1   *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 Symbol Configuration template file (i.e., MC9090.sct).
Get Defaults from Device	Load all parameter values from the current device.
Export Changes to .reg	Export the changed parameter values to an reg file.
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 .reg	Export all the parameter values to an reg 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 SCM.
Device Menu	
Device type	Change the current device type template. Each template (available from the Support Central) must reside in the SCM directory.
Tools Menu	
Signing Wizard	Adds a digital signature to a file.
Reg File Conversion Wizard	Converts a .reg file into a cpl or cab file.
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 8-2* for a particular parameter:

Table 8-2   *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 8-3* from left to right:

Table 8-3   *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.
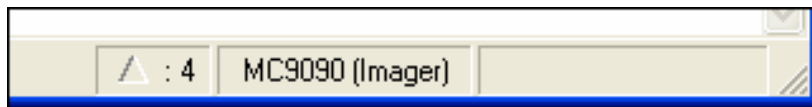
Figure 8-2   *Sample Status Bar*

The sample status bar in *Figure 8-2* shows that the current configuration file contains 3 modified parameters.

File Deployment

The .reg file created by the SCM export function must be deployed to the mobile computer.

1. Select **File** > **Export changes to .reg** to create a .reg file for only the changes made or select **File** > **Export all to .reg** to create a .reg file for all settings.

2. Copy the .reg file to the mobile computer.

3. Tap the filename to install.

4. Certain applications and settings require a cold boot to take affect. In these cases, cold boot the mobile computer. Refer to the *Windows Mobile Version 5.0 Help* file for more information.

Symbol Mobility Developer Kits

The Symbol Mobility Developer Kit (SMDK) family of products allows you to write applications that take advantage of the capture, move and manage capabilities of Symbol mobile computers. Go to the Support Central to download the appropriate developer kit.

Chapter 9 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** Windows CE OEM version 01.22.0001 and lower use MSP 2.X RD Client version 1.9.0.
> Windows Mobile OEM version 01.35.0002 and lower use MSP 2.X RD Client version 1.9.0.
> Windows CE OEM version 01.26.0001 and higher use MSP 3.X RD Client version 3.28.
> Windows Mobile OEM version 02.39.0001 and higher use MSP 3.X RD Client version 3.28.

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
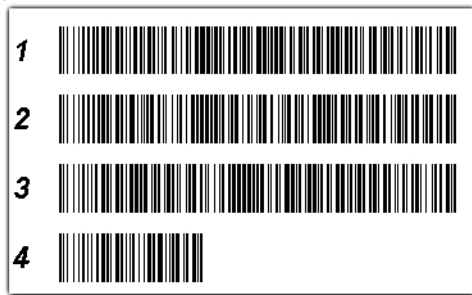
Figure 9-1   *RD Bar Code Printout Sample*

To access the **Rapid Deployment** window tap > **Programs** > **Rapid Deployment Client**.
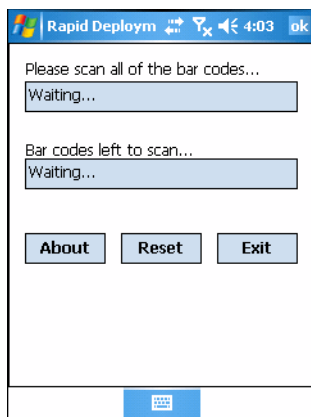
Figure 9-2   *Rapid Deployment Window (Version 1.9.0)*

Table 9-1   *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 9-22* 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.

Ready to Scan
No Bar Codes Left to Scan

Ready to Scan
Bar Codes Left to Scan are Listed
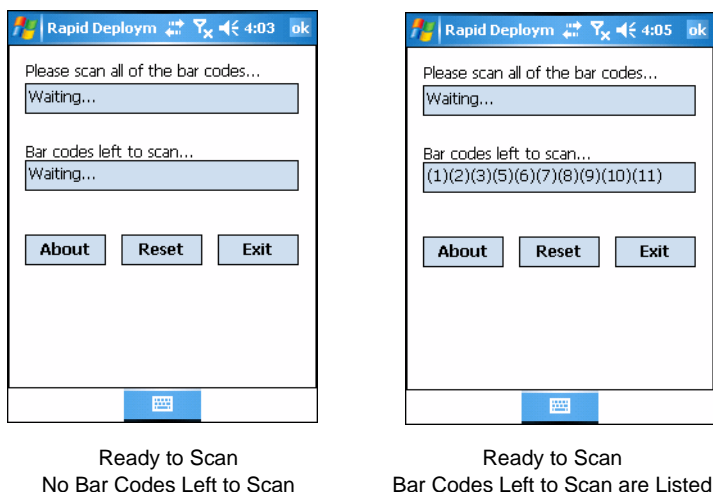
Figure 9-3   *Rapid Deployment Window*

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 9-7*).

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.
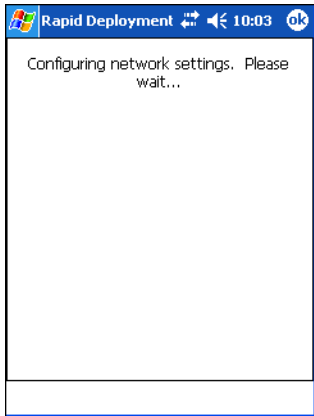
Figure 9-4   *Rapid Deployment Window - Configuring*

> **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 8, Wireless Applications for more information about wireless profiles.

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

RD Client Version 3.28

The RD Client version 3.28 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.
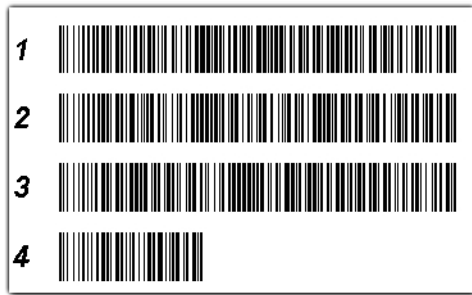
Figure 9-5   *RD Bar Code Printout Sample*

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.
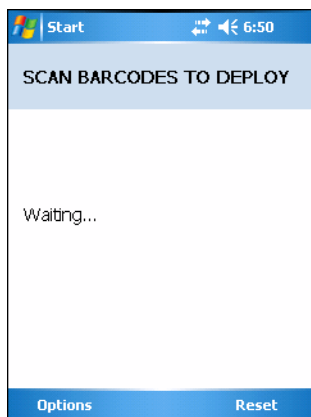
Figure 9-6   *Waiting for Bar Codes*

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.
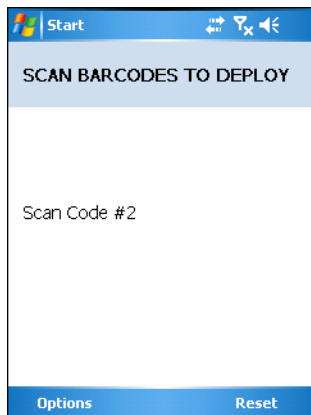
Figure 9-7   *Rapid Deployment Window*

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.
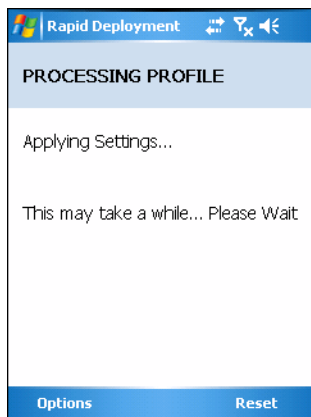
Figure 9-8   *Rapid Deployment Window - Processing Profile*

5.   When staging is complete the **STAGING COMPLETE** window displays.
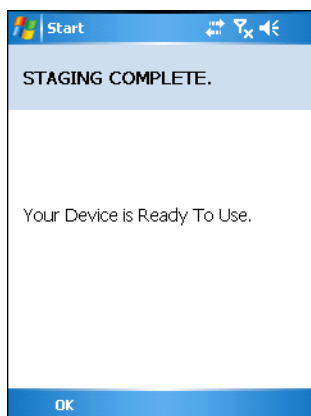
Figure 9-9   *Staging Complete Window*

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 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 Motorola WLAN adapters. The **RD Client** attempts to configure and establish WLAN IP connections using pre-defined Motorola 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.
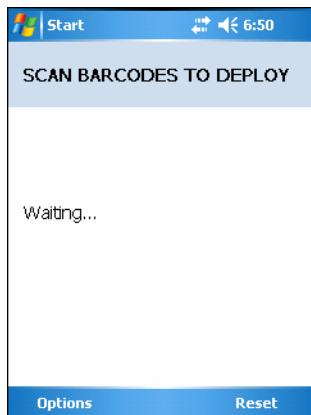
Figure 9-10   *Waiting for Bar Codes*

2. Press the left function key to select **Options**. The **Main Menu** window appears.
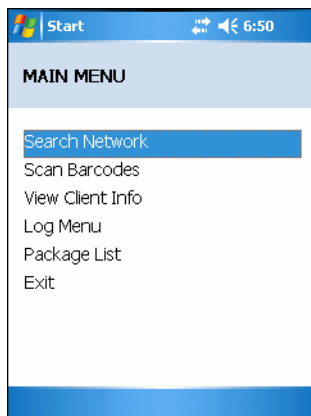
Figure 9-11   *RD Client Main Menu*

3. Use the up/down arrow keys to select **Search Network** and then press the center function key. The **SEARCHING NETWORKS** window appears.
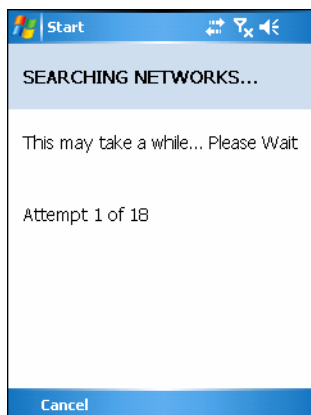
Figure 9-12   *RD Client Searching for On-Demand Profile Server*

4. When complete, the **STAGING COMPLETE** window displays.
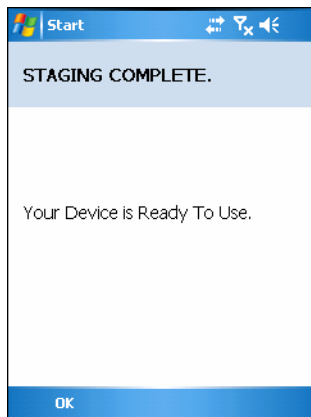
Figure 9-13   *Staging Complete Window*

Press the left function key to exit.

RD Client Main Menu

The RD Client **Main Menu** contains the following options:

- Search Network. See *On-Demand Staging on page 9-7* for detailed information.
- Scan Barcodes See *Bar Code Scanning on page 9-5* for detailed information.
- View Client Info
- Log Menu
- Package List
- Exit - Closes the RD Client application.
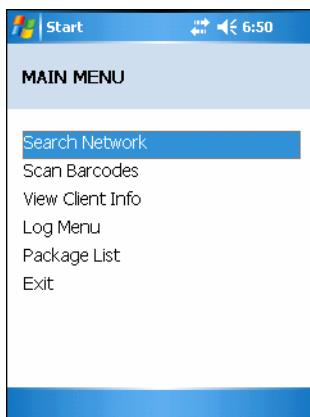
Figure 9-14   *RD Client Main Menu*

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.

Figure 9-15   *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.
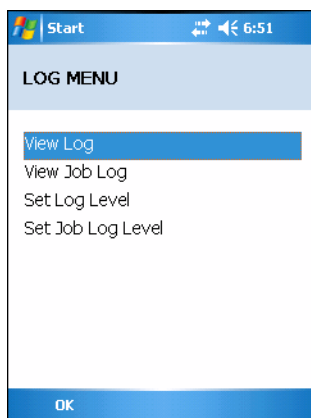
Figure 9-16   *Log Menu Window*

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.
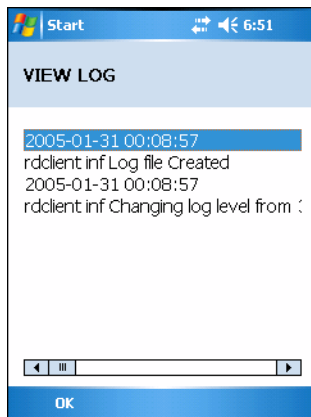
Figure 9-17   *View Log Window*

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.
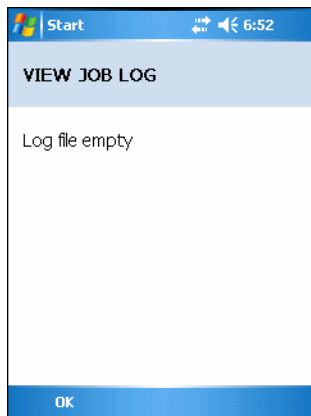
Figure 9-18   *View Job Log Window*

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.

Figure 9-19   *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 9-20   *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.
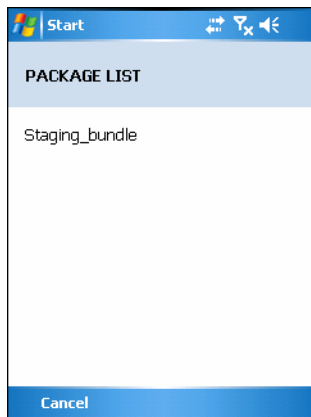
Figure 9-21   *Package List Window*

Tap **OK** to return to the **Main Menu**.

Provisioning

The MC90X 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.
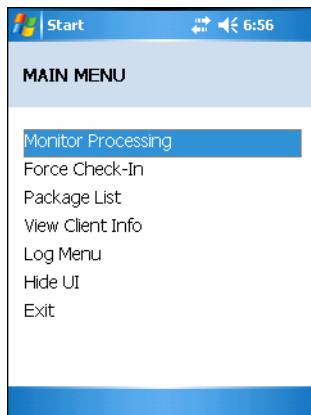
Figure 9-22   *MSP Agent Main Menu*

Monitor Processing

Use the **Monitor Processing** option to view the status of packages being processed.

Select the **Monitor Processing** option.
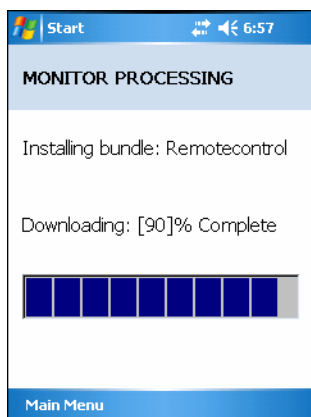
Figure 9-23   *Monitor Processing Window*

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.
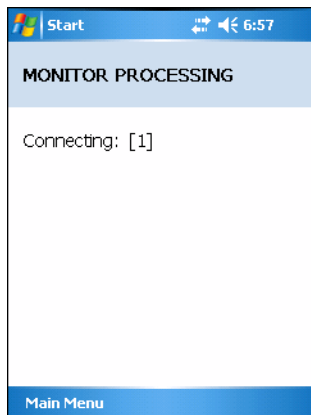
Figure 9-24   *Force Check-in Window*

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.
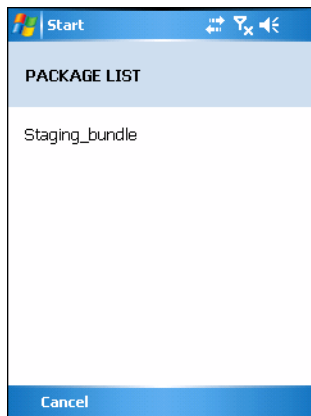
Figure 9-25   *Package List Window*

Tap **OK** to return to the **Main Menu**.
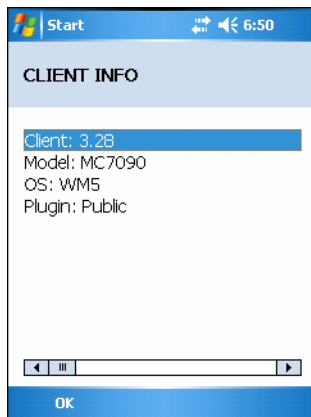
Client Info

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.
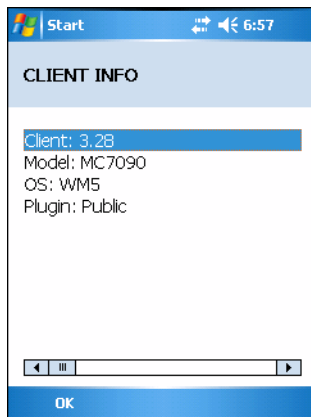
Figure 9-26   *Client Info Window*

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.
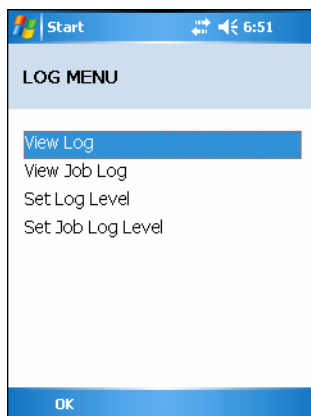
Figure 9-27   *Log Menu Window*

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.
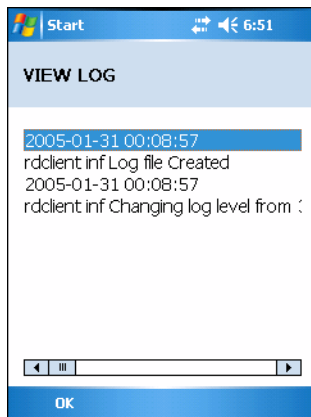
Figure 9-28   *View Log Window*

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.
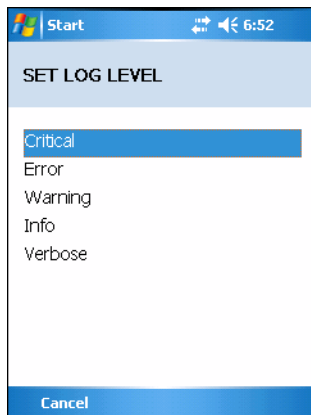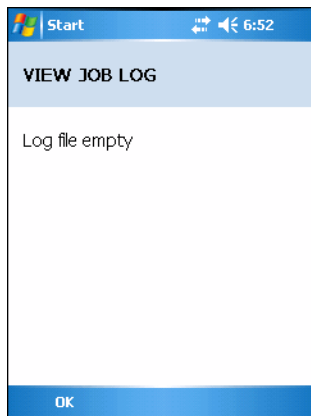

Figure 9-29   *View Job Log Window*

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.
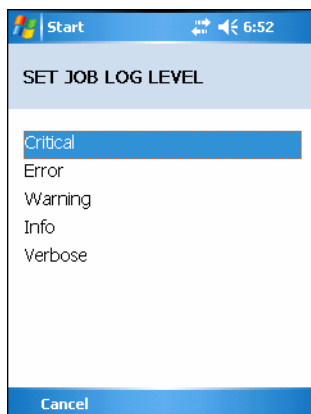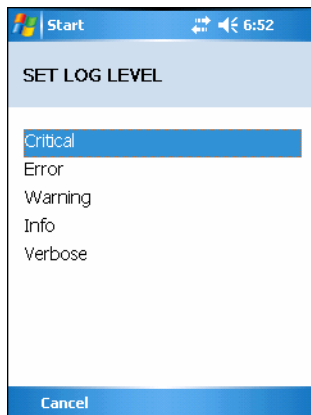
Figure 9-30   *Set Log Level Window*

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.
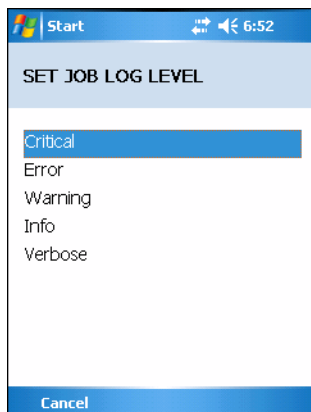
Figure 9-31   *Set Job Log Level Window*

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.
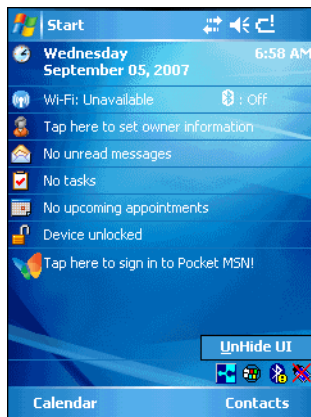
Figure 9-32   *UnHide UI Selection*

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 9-33   *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.
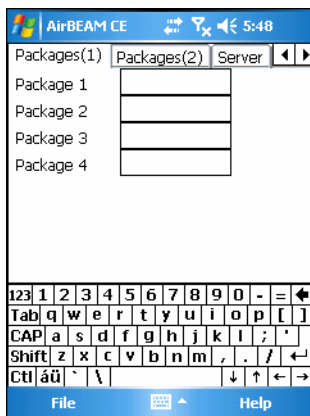
Figure 9-34   *Package (1) Tab*

Table 9-2   *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.

Table 9-2 *Package (1) Tab Descriptions (Continued)*

Field	Description
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.
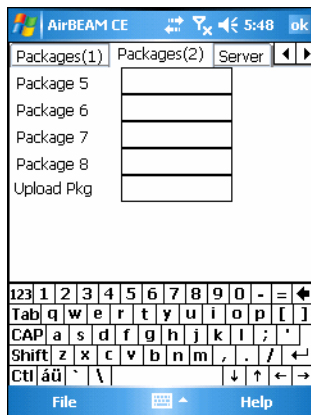
Figure 9-35 *Package (2) Tab*

Table 9-3 *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 9-36   *Server Tab*

Table 9-4   *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.
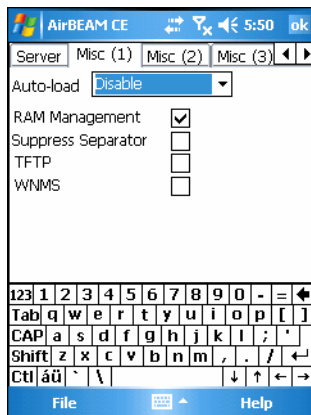
Figure 9-37   *Misc (1) Tab*

Table 9-5   *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.
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.

Table 9-5   *Misc(1) Tab Descriptions (Continued)*

Field	Description
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.

Figure 9-38   *Misc (2) Tab*

Table 9-6   *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.

Table 9-6   *Misc(2) Tab Descriptions (Continued)*

Field	Description
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.
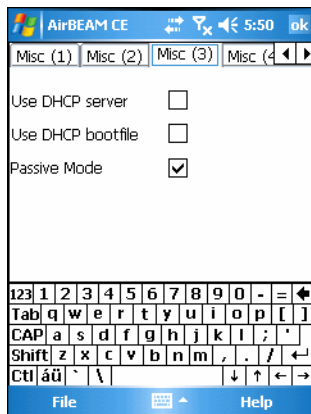
Figure 9-39   *Misc (3) Tab*
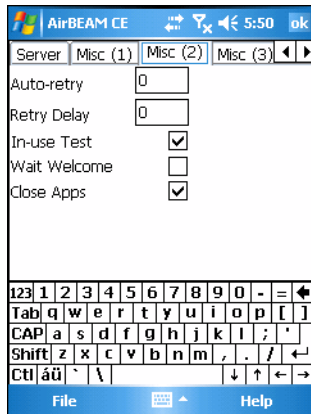
Table 9-7   *Misc (3) Tab Descriptions*

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.
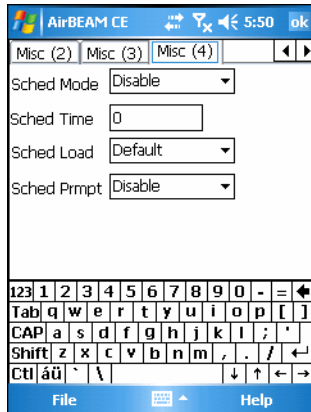
Figure 9-40   *Misc (4) Tab*

Table 9-8   *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 9-8 *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 9-22*.

2. From the main *AirBEAM CE* window, press **ALT** - **ALT** and select **Synchronize**.

3. Once connected, the AirBEAM Synchronize window appears.
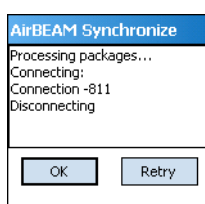
Figure 9-41 *AirBEAM Synchronize Window*

- 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 9-25*). 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 9-25* for instructions on enabling Auto Sync.

Chapter 10 Maintenance & Troubleshooting

Introduction

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

Maintaining the Mobile Computer

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

- Take care not to 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 an actual 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 you would a pocket calculator or other small electronic instrument.

- The touch-sensitive screen of the mobile computer contains glass. Take care 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 Motorola Enterprise Mobility support. See *Service Information on page xxi* 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, call Motorola Enterprise Mobility support to arrange for inspection. See *Service Information on page xxi* for contact information.

Troubleshooting

Mobile Computer

Table 10-1   *Troubleshooting the Mobile Computer*

Problem	Cause	Solution
Mobile computer does not turn on.	Lithium-ion battery not charged.	Charge or replace the lithium-ion battery in the mobile computer.
	Lithium-ion battery not installed properly.	Ensure battery is installed properly. See *Installing and Removing the 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. See *Resetting the Mobile Computer on page 1-12*.
Rechargeable lithium-ion battery did not charge.	Battery failed.	Replace battery. If the mobile computer still does not operate, try a warm boot, then a cold boot. See *Resetting the Mobile Computer on page 1-12*.
	Mobile computer removed from cradle while battery was charging.	Insert mobile computer in cradle and begin charging. The lithium-ion battery requires less than four hours to recharge fully.
Cannot see characters on display.	Mobile computer not powered on.	Press the **Power** button.
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 Synchronization cable and re-transmit.
	Incorrect cable configuration.	See the System Administrator.
	Communication software was incorrectly installed or configured.	Perform setup. See *Chapter 2, Accessories* for details.
		Ensure that Microsoft ActiveSync 4.1 or greater is installed on the host computer.

Table 10-1   *Troubleshooting the Mobile Computer (Continued)*

Problem	Cause	Solution
No sound is audible.	Volume setting is low or turned off.	Unit may be a beeper only unit or incorrect Config Block is programmed into device.
Mobile computer turns itself off.	Mobile computer is inactive.	The mobile computer turns off after a period of inactivity. If the mobile computer is running on battery power, this period can be set to 30 sec., 1, 2, 3, 4, 5 or 6 minutes. If the mobile computer is running on external power, this period can be set to 1, 2, 3, 5, 10, 15 and 30 minutes. For Windows Mobile 5.0 devices, Check the power settings by tapping **Start** > **Settings** > **System** tab > **Power** icon > **Advanced** tab. For WinCE 5.0 devices, Check the power settings by tapping **Start** > **Settings** > **Control Panel** > **Power** icon > **Power Off** tab. Change the setting if you need a longer delay before the automatic shutoff feature activates.
	Battery is depleted.	Replace the battery.
	Battery is not inserted properly.	Insert the battery properly (see *Installing and Removing the Main Battery on page 1-6*).
Tapping the window buttons or icons does not activate the corresponding feature.	LCD screen not aligned correctly.	Re-calibrate the screen.
	The system is hung.	Warm boot the system. To perform a warm boot (see *Resetting the Mobile Computer on page 1-12*).
A message appears stating that the mobile computer memory is full.	Too many files stored on the mobile computer.	Delete unused memos and records. You can save these records on the host computer.
	Too many applications installed on the mobile computer.	If you have installed additional applications on the mobile computer, remove them to recover memory. For Windows Mobile 5.0 devices, tap **Start** > **Settings** > **System** tab > **Remove Programs** icon. For WinCE 5.0 devices, tap **Start** > **Settings** > **Control Panel** > **Remove Programs** icon. Select the unused program and tap **Remove.**

Table 10-1   *Troubleshooting the Mobile Computer (Continued)*

Problem	Cause	Solution
The mobile computer does not accept scan input.	Scanning application is not loaded.	Verify that the unit is loaded with a scanning application. See the System Administrator.
	Unreadable bar code.	Ensure the symbol is not defaced.
	Distance between exit window and bar code is incorrect.	Ensure mobile computer is within proper scanning range.
	Mobile computer is not programmed for the bar code.	Ensure the mobile computer is programmed to accept the type of bar code being 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.	If the scanner stops emitting a laser beam when the trigger is pressed, check the battery level. When the battery is low, the scanner shuts off before the mobile computer low battery condition notification. Note: If the scanner is still not reading symbols, contact the distributor or Symbol Technologies.

Bluetooth Connection

Table 10-2   *Troubleshooting Bluetooth Connection*

Problem	Cause	Solution
Mobile computer cannot find any Bluetooth devices nearby.	Too far from other Bluetooth devices.	Move closer to the other Bluetooth device(s), within a range of 10 meters.
	The Bluetooth device(s) nearby are not turned on.	Turn on the Bluetooth device(s) you wish to find.
	The Bluetooth device(s) are not in discoverable mode.	Set the Bluetooth device(s) to discoverable mode. If needed, refer to the device's user documentation for help.

Table 10-2   *Troubleshooting Bluetooth Connection (Continued)*

Problem	Cause	Solution
Mobile computer keeps powering down to protect memory contents.	The mobile computer's battery is low.	Recharge the battery.
When trying to connect a Bluetooth phone and mobile computer, the phone thinks a different mobile computer (that I previously paired with the phone) is used.	The phone remembers the name and address of the mobile computer it last paired with via the Bluetooth radio.	Manually delete the pairing device and name from the phone. Refer to the phone's user documentation for instructions.
There is a delay in the Bluetooth stack re-initializing during a resume from suspend.	This is the normal behavior.	No solution required.

Four Slot Charge Only Cradle

Table 10-3   *Troubleshooting the Four Slot Charge Only Cradle*

Problem	Cause	Solution
Mobile computer charge indicator LED does not light.	Cradle is not receiving power.	Ensure the power supply is securely connected and receiving power.
	Mobile computer is not seated correctly in the cradle.	Ensure the battery is properly installed in the mobile computer, and re-seat the mobile computer in the cradle.
	The battery is not properly installed in the mobile computer.	
	The battery in the mobile computer is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
Note: The Four Slot Charge Only Cradle has no power indication.		

Four Slot Ethernet Cradle

Table 10-4 *Troubleshooting the Four Slot Ethernet Cradle*

Symptom	Cause	Solution
Attempt by the mobile computer to ActiveSync failed.	Cannot perform ActiveSync connection.	ActiveSync over an Ethernet connection is not available with Microsoft Mobile 5.0 or Microsoft CE 5.0 and ActiveSync 4.1.
During communications, no data was transmitted, or transmitted data was incomplete.	Mobile computer removed from cradle during communications.	Replace mobile computer in cradle and retransmit.
	Mobile computer has no active connection.	An icon will be visible in the status bar if a connection is currently active.
Mobile computer has successfully connected through the cradle, but no data is being transmitted over the connection.	Data is being transferred over the wireless link.	Temporarily disable the radio link to force data transmission through the cradle. Tap the wireless LAN icon from the systray on the Today screen. Tap the *Mode/General* tab. Enter an in-valid value in the *ESSID:* text box and tap the OK button. Power cycle the mobile computer. Verify that your radio link has been disabled (the wireless LAN icon has a red box with a "!" on it). Once you have completed your data transmission, re-enable your radio link.
All Communication Status LEDs are flashing red.	The unit could not configure itself, or it has lost the lease on its IP address.	Connect the unit to an Ethernet network with a correctly functioning DHCP server.
	Failed automatic cradle configuration via local DHCP service.	Connect a properly configured DHCP server or DHCP relay agent to the subnet, and power cycle the cradle. Check the DHCP server log to verify that the cradle is receiving a response to its DHCP request.
	The Ethernet link may be down.	Ensure the ethernet cable is connected to an active hub.
Communication Status LED does not light up.	Mobile computer has been inserted incorrectly into the cradle.	Remove, wait a minute, and then reinsert the mobile computer, ensuring it fits snugly onto the connector at the bottom of the cradle.
	Cradle is not receiving power.	Ensure the power supply is securely connected and receiving power.

Table 10-4   *Troubleshooting the Four Slot Ethernet Cradle (Continued)*

Symptom	Cause	Solution
Battery is not recharging.	Mobile computer removed from the cradle too soon.	Replace the mobile computer into the cradle. It can take up to four hours to recharge a completely depleted battery pack if mobile computer is suspended or longer if the mobile computer is on. For Windows Mobile 5.0 devices, view battery status by tapping **Start** > **Settings** > **System** tab > **Power** icon. For WinCE 5.0 devices, view battery status by tapping **Start** > **Settings** > **Control Panel** > **Power** icon.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	Mobile computer is not inserted correctly into the cradle.	Remove the mobile computer and reinsert it correctly. Verify charging is active. For Windows Mobile 5.0 devices, view battery status by tapping **Start** > **Settings** > **System** tab > **Power** icon. For WinCE 5.0 devices, view battery status by tapping **Start** > **Settings** > **Control Panel** > **Power** icon.
Warning Message - "! Unable to obtain a server assigned IP address. Try again later or enter an IP address in Network Settings."	This message occurs if a suspend/resume cycle is performed and the mobile computer radio is not associated (e.g. due to being out of range)	Tap 0K to close the message. The mobile computer will obtain address information and communicate through the ethernet cradle.

Four Slot Spare Battery Charger

Table 10-5   *Troubleshooting The Four Slot Spare Battery Charger*

Symptom	Possible Cause	Action
Batteries not charging.	Battery was removed from the charger or charger was unplugged from AC power too soon.	Ensure MSR is receiving power. Ensure mobile computer is attached correctly. Confirm main battery is charging. If a mobile computer battery is fully depleted, it can take up to four hours to fully recharge a battery (if the mobile computer is off and longer if the mobile computer is operating). For Windows Mobile 5.0 devices, view battery status by tapping **Start** > **Settings** > **System** tab > **Power** icon. For WinCE 5.0 devices, view battery status by tapping **Start** > **Settings** > **Control Panel** > **Power** icon.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	Battery contacts not connected to charger.	Verify that the battery is seated in the battery well correctly with the contacts facing down.

Single Slot Serial/USB Cradle

Table 10-6   *Troubleshooting the Single Slot Serial/USB Cradle*

Symptom	Possible Cause	Action
LEDs do not light when mobile computer or spare battery is inserted.	Cradle is not receiving power.	Ensure the power cable is connected securely to both the cradle and to AC power.
	Mobile computer is not seated firmly in the cradle.	Remove and re-insert the mobile computer into the cradle, ensuring it is firmly seated.
	Spare battery is not seated firmly in the cradle.	Remove and re-insert the spare battery into the charging slot, ensuring it is firmly seated.
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. Confirm main battery is charging. If a mobile computer battery is fully depleted, it can take up to four hours to fully recharge a battery (if the mobile computer is off and longer if the mobile computer is operating). For Windows Mobile 5.0 devices, view battery status by tapping **Start** > **Settings** > **System** tab > **Power** icon. For WinCE 5.0 devices, view battery status by tapping **Start** > **Settings** > **Control Panel** > **Power** icon.
	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 firmly seated.
Spare battery is not charging.	Battery not fully seated in charging slot.	Remove and re-insert the spare battery into the cradle, ensuring it is firmly seated.
	Battery inserted incorrectly.	Ensure the contacts are facing down and toward the back of the cradle.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
During data communications, no data was transmitted, or transmitted data was incomplete.	Mobile computer removed from cradle during communications.	Replace mobile computer in cradle and retransmit.
	Incorrect cable configuration.	See the System Administrator.
	Communications software is not installed or configured properly.	Perform setup as described in *Chapter 2, Accessories*.
		Ensure that Microsoft ActiveSync 4.1 or greater is installed on the host computer.

Vehicle Cradle

Table 10-7   *Troubleshooting The Vehicle Cradle*

Symptom	Possible Cause	Action
Mobile computer battery charging LED does not light.	Cradle is not receiving power.	Ensure the power input cable is securely connected to the cradle's power port.
Mobile computer's battery is not recharging.	Mobile computer was removed from the cradle too soon.	Replace the mobile computer in the cradle. If the mobile computer's battery pack is fully depleted, it can take four hours to fully recharge the battery.
	Battery is faulty.	Replace the battery.
	Mobile computer was not placed correctly in the cradle.	Remove the mobile computer from the cradle, and re-insert correctly. If the battery still does not charge, contact Customer Support. The mobile computer battery charging LED blinks amber when the mobile computer is correctly inserted and is charging.
No data was transmitted, or transmitted data was incomplete.	Mobile computer was removed from the cradle during communication.	Replace the mobile computer in the cradle and retransmit.
	The external device required a null modem cable, which was not used.	Retransmit using a null modem cable.
	Incorrect cable configuration.	See the System Administrator.

Cable Adapter Module

Table 10-8 *Troubleshooting The Cable Adapter Module*

Symptom	Possible Cause	Action
Mobile computer battery is not charging.	Mobile computer was removed from CAM or CAM was unplugged from AC power too soon.	Ensure CAM is receiving power. Ensure mobile computer is attached correctly. Confirm main battery is charging. If a mobile computer battery is fully depleted, it can take up to four hours to fully recharge a battery (if the mobile computer is off and longer if the mobile computer is operating). For Windows Mobile 5.0 devices, view battery status by tapping **Start** > **Settings** > **System** tab > **Power** icon. For WinCE 5.0 devices, view battery status by tapping **Start** > **Settings** > **Control Panel** > **Power** icon.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	The mobile computer is not fully attached to the CAM.	Detach and re-attach the CAM to the mobile computer, ensuring it is firmly connected.
During data communications, no data was transmitted, or transmitted data was incomplete.	Mobile computer detached from CAM during communications.	Re-attach mobile computer to CAM and retransmit.
	Incorrect cable configuration.	See the System Administrator.
	Communications software is not installed or configured properly.	Perform setup as described in *Chapter 2, Accessories.*

Magnetic Stripe Reader

Table 10-9 *Troubleshooting the Magnetic Stripe Reader*

Symptom	Possible Cause	Action
MSR cannot read card.	Mobile computer detached from MSR during card swipe.	Re-attach mobile computer to MSR and reswipe the card.
	Faulty magnetic stripe on card.	See the System Administrator.
	MSR application is not installed or configured properly.	Ensure the MSR application is installed on the mobile computer. Ensure the MSR application is configured correctly.

Table 10-9 *Troubleshooting the Magnetic Stripe Reader (Continued)*

Symptom	Possible Cause	Action
Mobile computer battery is not charging.	Mobile computer was removed from MSR or MSR was unplugged from AC power too soon.	Ensure MSR is receiving power. Ensure mobile computer is attached correctly. Confirm main battery is charging. If a mobile computer battery is fully depleted, it can take up to four hours to fully recharge a battery (if the mobile computer is off and longer if the mobile computer is operating). For Windows Mobile 5.0 devices, view battery status by tapping **Start** > **Settings** > **System** tab > **Power** icon. For WinCE 5.0 devices, view battery status by tapping **Start** > **Settings** > **Control Panel** > **Power** icon.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	The mobile computer is not fully attached to the MSR.	Detach and re-attach the MSR to the mobile computer, ensuring it is firmly connected.
During data communications, no data was transmitted, or transmitted data was incomplete.	Mobile computer detached from MSR during communications.	Reattach mobile computer to MSR and retransmit.
	Incorrect cable configuration.	See the System Administrator.
	Communications software is not installed or configured properly.	Perform setup as described in *Chapter 2, Accessories.*

Modem Module

Table 10-10 *Troubleshooting the Modem Module*

Symptom	Possible Cause	Action
Mobile computer is not communicating through the modem.	The modem cable is not fully connected.	Connect the modem cable securely to both the modem and the telephone jack.
	Modem is not securely connected to the mobile computer.	Reconnect the modem firmly to the mobile computer.
	Communication software is not installed or configured properly.	Set up the communication software as described in the mobile computer's *Product Reference Guide.*
	Problem in the telephone lines.	Connect a conventional telephone and dial the remote modem to verify the telephone lines are functioning. If the remote modem does not answer the call and emit answering tones, contact the remote System Administrator.
	Mobile computer's battery is low or discharged, which shuts off power to the modem.	Install a charged battery in the mobile computer, or use an external DC power adapter to recharge the battery.
ActiveSync fails.	A partnership was not established with the host computer.	Establish a partnership with the host computer (see *Chapter 2, Accessories*).
	Host computer is not selected in the *ActiveSync* window on the mobile computer.	Select a host computer in the *ActiveSync* window, and perform setup (see *Chapter 2, Accessories*).
	Modem RAS connection not allowed by host computer.	Select RAS connection in the host computer *(File - Connection Settings* window). Refer to the ReadMe files located in the Microsoft ActiveSync folder on the host computer.
	Mobile computer or modem was disconnected from the telephone line while ActiveSync was in progress.	Disconnect the modem cable for 30 seconds to hang up the local telephone connection. Close any open windows on the mobile computer and any modem connections.
	Synchronization occurred, but the session is configured to close immediately after synchronization is complete.	Verify the setting of the *When manually synchronizing disconnect when complete* checkbox by tapping *Start - ActiveSync - Tools - Options - Schedule* tab.

Table 10-10 *Troubleshooting the Modem Module (Continued)*

Symptom	Possible Cause	Action
Dial-out fails	Location setting is incorrect.	Verify Dialing Locations. Verify Dialing Patterns are correct for the current location. For example, enter 'G' in the *For local calls, dial:* field to dial directly, or '9,G' if the telephone system requires dialing '9' first to access an outside line.
	Incorrect server phone number.	Verify the connection phone number in the *Connecting* window.
	Pulse dialing not supported for country.	Use a connection within a tone-dialing system.
	Dialtone detection not supported.	The service you subscribe to (e.g., a remote answering service) may use a different type of dialtone. Disable dialtone detection on the modem by entering the initialization string "ATXO" in the *Extra dial-string modem commands:* text box of the *Modem Settings* window.
	The Connection Manager routes are incorrect.	Warm boot the mobile computer and confirm the connection settings.

Appendix A Technical Specifications

Technical Specifications

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

Mobile Computer

The following table summarizes the mobile computer's technical specifications.

Table A-1 *Technical Specifications*

Item	MC909X-G	MC909X-K	MC909X-S
Physical and Environmental Characteristics			
Dimensions (Non-WAN)	9.1 in. L x 3.6 in. W x 7.6 in. H 23.1 cm L x 9.1 cm H x 19.3 cm H	9.1 in L x 3.6 in. W x 2.2 in. H 23.1 cm L x 9.1 cm H x 5.6 cm H	7.9 in L x 3.6 in. W x 2.2 in. H 20.1 cm L x 9.1 cm H x 5.6 cm H
Dimensions (WAN)	N/A	9.1 in L x 3.6 in. W x 2.3 in. H 23.1 cm L x 9.1 cm H x 5.8 cm H	7.9 in L x 3.6 in. W x 2.3 in. H 20.1 cm L x 9.1 cm H x 5.8 cm H
Weight	25 oz.(includes battery, scanner and radio)	22-25 oz., configuration-dependent	20-23 oz., configuration-dependent
Keyboard	28-key; 43-key; 53-key Terminal Emulation (5250, 3270, VT)	28-key; 33-key, 43-key; 53-key	28-key; 38-key alpha-prime; 38-key numeric-prime
Display	3.8 in. 1/4 VGA Monochrome or Color: Win CE (WM Color only)	3.8 in. 1/4 VGA Color	3.8 in. 1/4 VGA Color
Power	Removable, rechargeable 7.2 V Lithium Ion 2200 mAh battery pack, 15.8 watt hours	Removable, rechargeable 7.4 V Lithium Ion 2200 mAh battery pack, 15.8 watt hours	Removable, rechargeable 7.2 V Lithium ion 1550 mAh battery pack, 11.1 watt hours

Table A-1   *Technical Specifications (Continued)*

Item	MC909X-G	MC909X-K	MC909X-S
Performance Characteristics			
CPU	XScale Bulverde PXA270 processor at 624MHz		
Operating System	Microsoft Windows CE 5.0 or Windows Mobile 5.0 Premium Edition	Microsoft Windows Mobile 5.0 Premium and Phone Editions	
Memory (RAM/ROM)	Windows CE: 64MB/64MB Windows Mobile: 64MB/128MB	Windows Mobile: 64MB/128MB	
Expansion	SD/MMC Card		
Application Development	PSDK, DCP and SMDK available through Symbol Developer Zone Web Site	SMDK available through Symbol Developer Zone Web Site	
Data Capture Options	1D Standard Range scan engine 1D Long Range scan engine Omni-directional 1D and 2D imaging engine reads symbologies and captures grayscale images and signatures with intuitive laser aiming.	1D Standard Range scan engine Omni-directional 1D and 2D imaging engine reads symbologies and captures grayscale images and signatures with intuitive laser aiming.	
User Environment			
Operating Temperature	-4°F to 122°F (-20°C to 50°C)		
Storage Temperature	-25°F to 160°F (-40°C to 70°C)		
Battery Charging Temperature	32 °F to 104 °F (0 °C to +40 °C) ambient temperature range.		
Humidity	5% to 95% non condensing		
Drop Specification	Multiple 6 ft.(1.8m) drops to concrete across operating temperature range		
Tumble	2,000 one-meter tumbles at room temperature (4,000 hits)		
Environmental Sealing	IP64 (electronic enclosure)		
ESD	+/-15kVdc air discharge +/-8kVdc direct discharge +/-8kVdc indirect discharge		

Table A-1   *Technical Specifications (Continued)*

Item	MC909X-G	MC909X-K	MC909X-S
WLAN Wireless Data Communications			
WLAN radio	Symbol 802.11a/b/g		
Operating Channels	Channel 8 - 169 (5040 - 5845 MHz) (4920 - 4980 MHz) Japan only Channel 1 - 13 (2412 - 2472 MHz) Channel 14 (2484 MHz) Japan only Actual operating frequencies depend on regulatory rules and certification agency		
Security	WEP (40 or 128 bit), TKIP, TLS, TTLS (MS-CHAP), TTLS (MS-CHAP v2), TTLS (CHAP), TTLS-MD5, TTLS-PAP, PEAP-TLS, PEAP (MS-CHAP v2), AES, LEAP, WPA, WPA2 (Fusion 2.5 only)		
Voice Communication (Windows Mobile 5.0 devices only)	Integrated Voice-over-IP ready (P2P, PBX, PPT), Wi-Fi -certified, IEEE 802.11a/b/g direct sequence wireless LAN		
Output Power	100mW U.S. and International		
Data Rate	802.11a: 54Mb per second 802.11b: 11Mb per second 802.11g: 54Mb per second		
Frequency Range	802.11a: 5 GHz; country-dependent 802.11b: 2.4 GHz; country-dependent 802.11g: 2.4 GHz; country-dependent		
Antenna	Internal		
WPAN Wireless Data Communications			
Bluetooth	Bluetooth Version 1.2 with BTExplorer (manager) included		

Table A-1   *Technical Specifications (Continued)*

Item	MC909X-G	MC909X-K	MC909X-S
Wireless WAN (WWAN) Data Communications			

EDGE/GPRS Radio Module	N/A	General features:
		  • Quad-Band GSM 850/900/1800/1900 MHz
		  • EDGE Multislot class 10
		  • GPRS Multislot class 12
		  • GSM release 99
		  • Output power:
		    • class 4 (2 W) for GSM850
		    • class 4 (2 W) for EGSM900
		    • class 1 (1 W) for GSM1800
		    • class 1 (1 W) for GSM1900
		Specification for fax:
		  • Group 3, class 1
		Specifications for data EDGE (E-GPRS):
		  • Multislot class 10
		  • Modulation and coding scheme MCS 1– 9
		  • Mobile station class B
		Specifications for data (GPRS):
		  • Multislot class 12
		  • Full PBCCH support
		  • Mobile station class B
		  • Coding scheme 1– 4
		Specifications for SMS:
		  • Via GSM or GPRS
		  • Point-to-point MO and MT
		  • Text and PDU mode
		  • SMS cell broadcast
		Specifications for voice:
		  • Half rate (HR)
		  • Full rate (FR)
		  • Enhanced full rate (EFR)
		  • Adaptive multi rate (AMR)	

iDEN Radio Module	N/A	Frequency Range:
		  • 800 - 900 MHz
		ANtenna:
		  • internal
		GPS-Enabled:
		  • 12 channel assisted GPS (aGPS)	

Table A-1 *Technical Specifications (Continued)*

Item	MC909X-G	MC909X-K	MC909X-S
Peripherals and Accessories			
Cradles	Single-slot and 4-slot cradles available		
Printers	Supports extensive line of Symbol approved printers, cables and accessories		
Charger	4-Slot universal battery charger		
Other Accessories	Cable Adapter Module; Magnetic Stripe Reader; Modem; Full set of holsters In accordance with the SymbolPlus partner program		
Regulatory			
Electrical Safety	Certified to UL60950-1, CSA C22.2 No. 60950-1, EN60950-1, IEC 60950-1		
RF & EMC	FCC PArt 2 (SAR), FCC Part 15, RSS210; EN 300 328 & EN 301 487, EN55022, EN55024	**MC9090:** FCC Part 2 (SAR), FCC Part 15, RSS210 B, EN 300 328, 301 489-1, 489-17 **MC9094:** FCC Part 2 (SAR), FCC Part 22, FCC Part 24, FCC Part 15, RSS210, EN 300 328, EN 301 489-1, 301 489-7, 301 489-17 **MC9097:** FCC Part 2 (SAR), FCC Part 15, FCC Part 90, RSS210	
Laser Safety	IEC Class2/FDA Class II in accordance with IEC60825-1/EN60825-1		

Table A-2 *Data Capture Options*

Item	Description		
Laser Decode Capability	Code 39 Codabar Interleaved 2 of 5 MSI UPC/EAN supplementals Webcode RSS Expanded	Code 128 Code 11 EAN-8 UPCA Coupon Code RSS-14	Code 93 Discrete 2 of 5 EAN-13 UPCE Trioptic 39 RSS Limited
	MC909X with Windows Mobile 5.0 and OEM Version 01.39.0001 and MC909X with Windows CE 5.0 and OEM Version 01.26.0001 and higher: Chinese 2 of 5		
Imaging Decode Capability	Code 39 Codabar Discrete 2 of 5 EAN-13 UPC/EAN supplementals Webcode Composite C Macro PDF-417 RSS Expanded Data Matrix US Planet Canadian 4-state	Code 128 Code 11 MSI UPCA Coupon Code TLC39 Micro PDF-417 (Macro) Micro PDF-417 RSS Limited Maxi Code UK 4-state Japanese 4-state	Code 93 Interleaved 2 of 5 EAN-8 UPCE Trioptic 39 Composite AB PDF-417 QR Code RSS-14 US Postnet Australian 4-state Dutch Kix
	MC909X with Windows Mobile 5.0 and OEM Version 01.39.0001 and MC909X with Windows CE 5.0 and OEM Version 01.26.0001 and higher: Chinese 2 of 5 USPS 4-state (US4CB) Aztec microQR		

Modem Module

Table A-3   *Environmental Parameters and Technical Hardware Specifications*

Item	Description
Asynchronous character format	Up to 10 bits, including data, start, stop, and parity bits
Asynchronous data rates	Transmission rate fallback through 300 bps
Chipset	Conexant SCM
Compatible public switched network jacks	RJ11
Dialing capability	Tone and rotary pulse
Line requirements	Public switched telephone network (PSTN) including international connections
Operating environment	Altitude: up to 20,000 ft. Humidity: 10% to 90% non-condensing
Operating temperature	Operating: 32° to 122^oF / 0° to 50^oC Storage: -4° to 149^oF / -20° to 65^oC
Operating modes	Asynchronous, full duplex, automatic and manual call originate
Performance	Line speed up to 33,600 bps HHC to modem speed (DTE speed) up to 57,600 bps V.42bis data compression V.42 LAPM error correction
Current consumption	100 mA active <10 mA sleep
Pulse dialing rate (except where prohibited under TBR-21 rules)	10 pulses per second Pulse dialing duty cycle: 39/61% (US) make-to-break ratio
Ringer equivalence	0.1 dBm
Standards & protocols	Bell 103, Bell 212A, Hayes AT command set, and ITU Vs. 17, 21, 22 A & B, 22bis, 23, 25bis, 27 ter, 29, 32, 32bis, 42bis
Tone detected	Dial, busy, ring back, modem answer tones. Blind dialing based on time-out periods available for incompatible tones.
AC Adapter	9V, 2 amp regulated AC/DC adapter allows unlimited modem use. Do NOT substitute an AC adapter; using an incorrect AC power supply causes electrical damage to the mobile computer and voids warranty.

Mobile Computer Pin-Outs
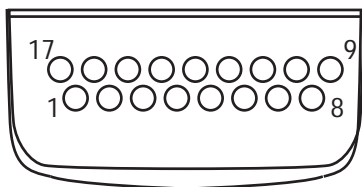
Figure A-1   *Pin Locations*

Table A-4   *Pin-Outs*

PIN Number	Signal Name	Function
1	USB_GND	USB
2	USB_D_PLUS	USB
3	TXD	RS232C
4	RXD	RS232C
5	DCD	RS232C
6	RTS	RS232C
7	DSR	RS232C
8	GND	Ground, 2.5A max.
9	RI	RS232C
10	CRADLE_DET	Grounded by cradle when in cradle
11	DTR	RS232C
12	Not connected	Not connected
13	POWER_IN	12V, 2.5A max
14	CTS	RS232C
15	USB_5V_DET	USB
16	USB_D_MINUS	USB
17	EXT_PWR_OUT	3.3V @500mA

Accessory CAM and MSR Pin-Outs
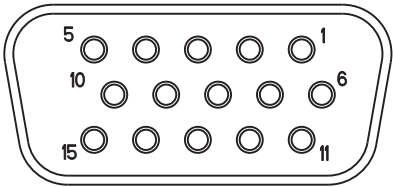
Figure A-2   *CAM and MSR Serial Connector*

Table A-5   *CAM and MSR Serial Connector Pin-outs*

Pin	Signal
1	USB_5V_DET
2	USB_D_MINUS
3	USB_D_PLUS
4	GND
5	GND
6	PWR_EXT_OUT
7	CRADLE_DET*
8	DSR
9	DCD
10	TXD
11	CTS
12	DTR
13	RI
14	RTS
15	RXD

Non-Incendive Devices

Hazardous (Classified) Location Class I, Division 2, Groups A, B, C & D
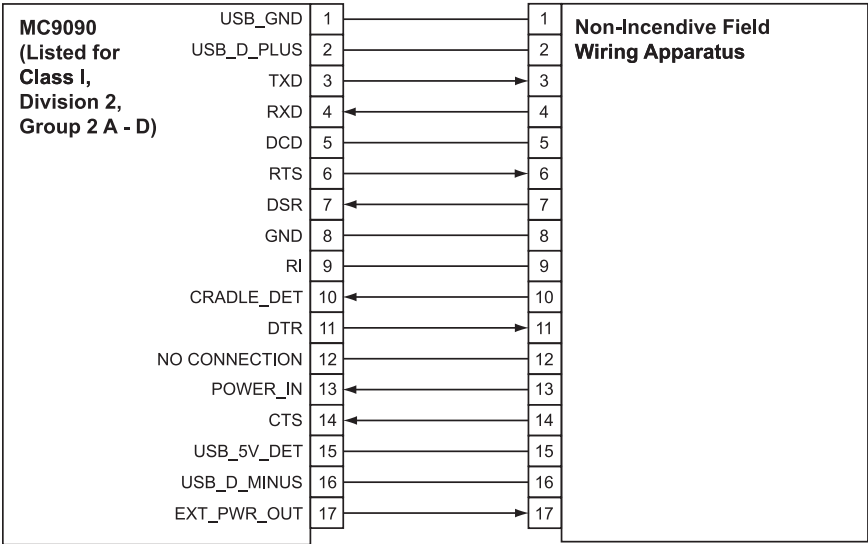
Pin 17 to Pin 8	Pins 3, 6, or 10 to Pin 8	Pin 17 to Pin 8	Pins 3, 6, or 10 to Pin 8
Vmax = 3.37 VDC	Vmax =5.6 VDC	Voc = 3.37 VDC	Voc =5.6 VDC
Imax = 850 mA	Imax = 31 mA	Isc = 850 mA	Isc = 31 mA
Ci = 100 µF	Ci = 200 µF	Ca = 73 µF	Ca = 200 µF
Li = 0.35 µH	Li = 100 µH	La = 12 µH	Li = 100 µH

Selected associated non-incendive field wiring apparatus shall satisfy the following:

Non-Incendive Field Wiring Apparatus		MC9090
Voc	$\leq$	Vmax
Isc	$\leq$	Imax
Ca	$\geq$	Ci
La	$\geq$	Li
Vmax	$\geq$	Voc
Imax	$\geq$	Isc
Ci	$\leq$	Ca
Li	$\leq$	La

Appendix B Using iDockIt

Introduction

iDockIt™ manages the activities that can occur when you connect the MC909X mobile computer to a host computer using a cradle (Ethernet, modem, serial, USB) or USB or serial cable. iDockIt can enable the mobile computer to connect automatically to a host computer, network, or the Internet and then exchange information or launch an application. iDockIt lets you establish settings for each type of connection.

This appendix provides an overview of configuring iDockIt on MC909X mobile computers running Windows Mobile 5.0 and Windows CE 5.0.

General iDockIt options let you:

- enable or disable iDockIt; if enabled, keep iDockIt running in the background.
- display status and cradle settings when you cradle the mobile computer.
- define whether iDockIt should wait before connecting or reconnecting the mobile computer to the host computer or network and if waiting, the number of seconds to delay.
- disable specific error dialogs.

Connection-specific options let you define what iDockIt should do when you cradle or connect the mobile computer, including:

- launch Microsoft ActiveSync to synchronize with a host computer.
- establish a connection to your network.
- launch an application after establishing a network connection.
- establish a connection via a specified modem.

> **NOTE** iDockIt settings and options control cradle events only while iDockIt is running.
>
> You cannot use ActiveSync 4.0 or later to synchronize data between a host computer and a Windows CE based device through an Ethernet cradle.

Configuring iDockIt for Windows Mobile 5.0

To run iDockIt for the first time, tap **Start** > **Programs** from the Today screen and then tap the **iDockIt** icon; iDockIt opens to the **General** tab. Thereafter, if you need to restart **iDockIt**, tap **Start** > **iDockIt** from the Today screen.

When **iDockIt** is running, you see its icon at the bottom of the Today screen. Tap the icon to display the iDockIt menu.
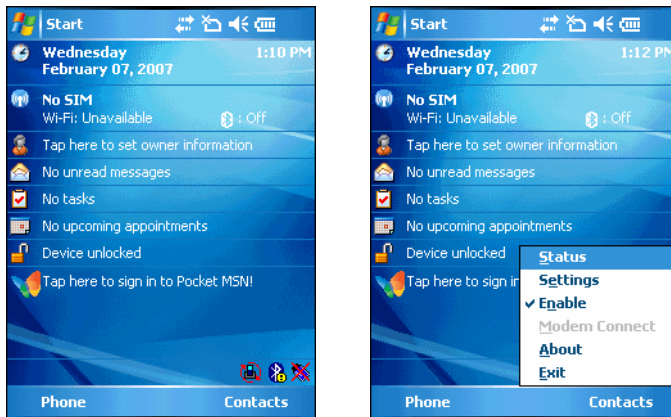
Figure B-1   *Today Screen showing iDockIt Menu*

- **Status** displays the **Status** tab.

- **Settings** displays the **Settings** tab for the current connection or, if the mobile computer is not connected to a host computer via a cable or cradle, the most recently viewed settings tab.

- **Enable** is a toggle switch that checks/unchecks the **Enable iDockIt** setting on the **General** tab.

- **Modem Connect** is enabled when you have defined a modem connection in the modem settings tab. Tapping this item when the mobile computer is in the modem cradle initiates dial-out.

- **About** displays version and copyright information.

- **Exit** disables iDockIt and closes the application.

iDockIt includes five tab pages:

- **General** - General setup options for enabling/disabling iDockIt and displaying status and other information.

- **Ethernet** - Settings for what iDockIt should do when it detects that the mobile computer is in an Ethernet cradle.

- **Direct** - Settings for what iDockIt should do when it detects that the mobile computer is in a Serial or USB cradle or connected to a host computer using a Serial or USB cable.

- **Modem** - Settings for what iDockIt should do when it detects that the mobile computer is in a Modem cradle.

- **Status** - Current connection status, continuously updated, scrollable window.

Quick Start

Follow these guidelines. Refer to sections of this appendix devoted to individual tabs for details on settings and options.

How To Start iDockIt

To start iDockIt the first time, tap **Start** > **Programs** > **iDockIt**. Thereafter, tap **Start** > **iDockIt**.

How To Enable iDockIt To Manage Connections

On the iDockIt **General** tab, check **Enable iDockIt** to enable iDockIt to control cradle events. When you cradle the mobile computer, iDockIt identifies the cradle and perform the activities you have configured for it.

To connect automatically to a host computer or network:

1.   Tap the iDockIt **General** tab.

2.   Check **Enable iDockIt**.

3.   **Check or uncheck Display status when cradled**.

4.   **Check or uncheck Display settings when cradled**; the **Autoconnect** setting is also optional.

5.   Tap the **iDockIt** tab that corresponds to your cradle type and check **Establish network connection** and optionally **Launch application**.

To connect manually to your host computer or network:

While iDockIt is designed to connect your mobile computer to a specified host computer or network automatically, you can also choose your connection manually whenever you place the mobile computer in the cradle.

1.   Tap the iDockIt **General** tab.

2.   Check **Enable iDockIt**.

3.   **Check or uncheck Display status when cradled**.

4.   Check **Display settings when cradled**. When you place the mobile computer in the cradle, the **Settings** tab displays automatically.

5.   Uncheck the **Autoconnect** option.

6.   Tap the **iDockIt** tab that corresponds to your cradle type.

7.   Check **Establish network connection** and optionally **Launch application**.

When you place the mobile computer in a cradle, iDockIt displays the **Settings** tab corresponding to that cradle. Choose the type of connection and tap . Another way to connect manually is to establish new connection settings before you place the mobile computer in the cradle.

To launch an application when you connect:

1.   Tap the iDockIt **General** tab.

2.   Check **Enable iDockIt**.

3.   Tap the tab that corresponds to the type of cradle you are using.

4.   Select a connection option as described above.

5.   Tap **Launch application**.

6.   Tap **Select** and select the application you want to launch when you place the mobile computer in the cradle. Enter any necessary program arguments.

7. Tap **OK**.

The selected application appears in the settings tab.

To determine the mobile computer's connection status:

Tap the iDockIt **Status** tab.

- **Dock Status** shows either **Docked** and identify the type of connection (Serial, Ethernet, USB) when the mobile computer is placed in the cradle or **Not docked** when the mobile computer is removed from the cradle.

- **Connection** shows the name of the connection,

- When the mobile computer is placed in the cradle, IP addresses shows all valid IP addresses assigned to the mobile computer. If the mobile computer is not in the cradle, this field shows either the IP address of the network adapter or, if you there is no network connection, a default IP address.

- The **Status** window shows all cradle events that have occurred since the last time the mobile computer was placed in the cradle.

Minimize iDockIt

To minimize iDockIt, tap **X** in the upper right corner of the window. iDockIt controls cradle events while it is minimized.

Exit iDockIt

To close the application, tap **File** > **Exit**. iDockIt does not control cradle events when it is closed.

General Setup Options

Settings on the **General** tab complement the options you set for your cradle.
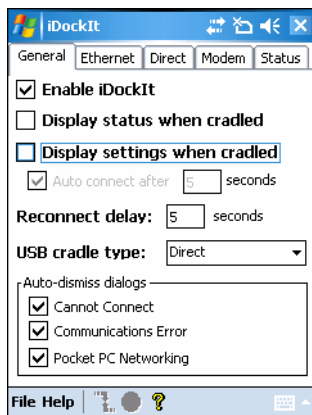
Figure B-2   *General Settings Tab*

Enable iDockIt

Check this option to enable iDockIt to control cradle events. When you place the mobile computer in a cradle, iDockIt identifies the type of cradle and perform the activities you have configured.

Display Status When Cradled

Check this option to display the iDockIt **Status** tab when you place the mobile computer in the cradle. If you also checked **Display** settings when cradled, you first see the **Settings** tab for the type of cradle detected and then the **Status** tab after the specified time elapses.

Display Settings When Cradled

Check this option to display the cradle settings tab when you place the mobile computer in the cradle. You can also check **Auto connect after x seconds** to automatically make the connection defined on the cradle tab after a specific delay. The delay gives you the opportunity to review/change connection options. During this waiting period, you can select either ![icon] or ![icon] in the menu bar to connect immediately or cancel automatic connection.

Warning If **Display settings when cradled** is checked and **Auto connect after** is not checked, iDockIt only displays the cradle settings tab when you cradle the mobile computer and does not attempt to connect to your network.

Reconnect Delay

If iDockIt is configured to establish a connection when cradled and the connection is lost, iDockIt attempts to re-establish the connection if the mobile computer is still cradled (external power from the cradle is present). The Reconnect delay is used to specify the number of seconds iDockIt should wait after a connection is lost before attempting to reconnect.

USB Cradle Type

When placed into a USB cradle, iDockIt needs to know whether the cradle directly connects to a host computer or if the cradle connects to your network via an Ethernet cable. If you are using iDockIt to synchronize with a host computer using ActiveSync via USB cable or cradle, select **Direct**.

If you are using iDockIt to connect to your network though an Ethernet cradle, select **Ethernet**.

Auto-dismiss Error Dialogs

You can configure iDockIt to dismiss several error messages that might be displayed as iDockIt makes the connection you have defined. These messages do not require any action. To auto-dismiss a message, tap the checkbox next to its title. If the message occurs during a connection attempt, iDockIt allows it on your behalf and the event appears in the **Status** window.

- **Cannot Connect** - The answering modem has disconnected. To check your connection settings and change them if needed, tap Settings.

  What this message means: This message may be displayed when you remove the mobile computer from a cradle, breaking the connection. Tapping Settings would display the Pocket host computer Connections dialog. Since you should not need to change these settings, the error message can be dismissed automatically.

- **Communications Error** - Cannot start communications with the desktop computer. Reconnect the mobile computer. If the problem persists, see Microsoft ActiveSync Help.

  What this message means: This message is displayed when ActiveSync® attempts to connect to a host computer and synchronize data but cannot find the computer name. Since this message may appear in the course of a successful connection attempt, it can be dismissed automatically.

- **Pocket host computer Networking** - Unable to obtain a server-assigned IP address. Try again later or enter an IP address in Network settings.

  What this message means: If the mobile computer has a wireless network adapter, this dialog may appear periodically when the mobile computer is out of network range. The message has nothing to do with your connection through a cradle or cable and can therefore be dismissed automatically.

Status Tab

If iDockIt is enabled when you cradle/connect the mobile computer, the **Status** tab displays connection-related events as they occur. To display this tab automatically whenever you cradle/connect the mobile computer, check **Display status when cradled** on the **General** tab.
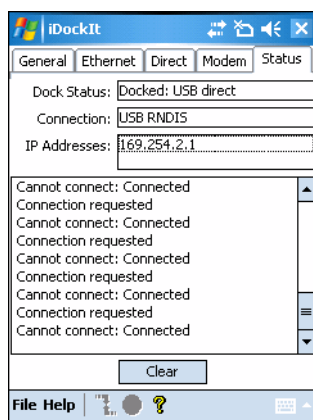
Figure B-3 *Status Tab*

The **Dock Status** field shows **Docked** and identifies the type of connection (Serial, Ethernet, USB) when you have cradled the mobile computer or **Not docked** when you remove the mobile computer from the cradle.

The **Connection** field shows the name of the connection.

When you have placed the mobile computer in the cradle, the **IP addresses** field shows all valid IP addresses assigned to the mobile computer. When the mobile computer is not cradled, this field shows either the IP address of your network adapter or, if you do not have a network connection, a default IP address.

The **Status** window displays a scrolling list of cradle events as they occur, including:

- AC power ON and OFF as you insert and remove the mobile computer.
- **Carrier detect**, baud rate, and **(cradle type) connect** when iDockIt identifies the cradle and connection speed.
- **Launch (application)** when iDockIt launches the selected application, followed by confirmation when the application has been launched successfully.
- **Sync done** when synchronization has completed successfully.
- **Dismiss (error message)** when iDockIt dismisses a message you have designated.
- **Dock event complete** when iDockIt has completed all defined tasks. If you remove the mobile computer from the cradle before this item appears, regardless of dock status, you may interrupt assigned tasks.

Tap **Clear** to empty all events from the **Status** tab.

Ethernet Cradle Settings

If using an Ethernet cradle, you can establish an Internet or Intranet connection to your network and/or launch a specified application on the mobile computer.

> **NOTE**   You cannot use ActiveSync 4.0 or later to synchronize data between a host computer and a Windows CE based device through an Ethernet cradle.
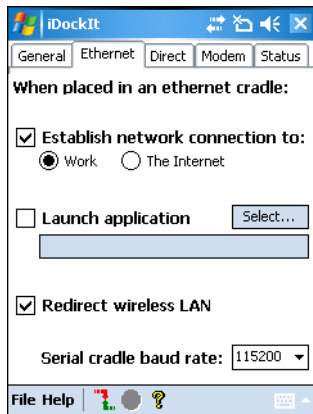
Figure B-4   *Ethernet Settings Tab*

Establish Network Connection

Check this option to have iDockIt establish a network connection when you cradle the mobile computer.

You can check this option in conjunction with **Launch application**. After iDockIt establishes the network connection, it launches the specified application.

Launch Application

Check this option to have iDockIt launch the selected application when you cradle the mobile computer. iDockIt uses the specified command line parameters. You must select an application to launch.

Select...

1. Tap **Select** to open the **Select Auto-Launch Application** dialog.

2. Select a **File Type** in the drop-down list.

3. Select a Folder (as needed).

4. Select a file name in the list.

5. Use the input panel to specify command line parameters.

6. Tap **OK** at the top of the screen.

The selected application appears in the settings tab.

Serial Cradle Baud Rate

This option allows you to specify the baud rate iDockIt should use for a serial connection to the Ethernet cradle. Set this rate to match the baud rate configured for the cradle. For maximum performance, always use the maximum baud rate of 115200.

If using a USB-to-Ethernet cradle, the USB driver automatically determines the connection speed.

Direct (Serial/USB) Settings

If you use a serial or USB cradle or connect to the mobile computer with a serial or USB cable, you can automatically synchronize with the connected host computer. Alternatively, if your host computer supports RAS connections you can connect to a network through a host computer and/or launch a specified application on the mobile computer.
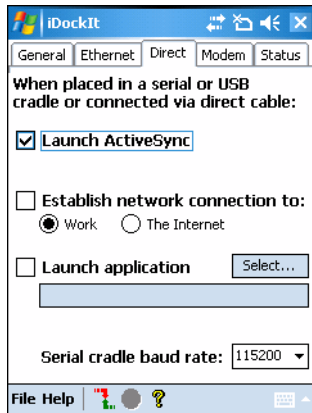
Figure B-5   *Direct (Serial/USB) Settings Tab*

Launch ActiveSync

Check this option to have iDockIt launch ActiveSync when you place the mobile computer in a serial or USB cradle or when you connect it to a serial or USB cable. If the mobile computer has a partnership with the host computer to which you are connected, ActiveSync automatically synchronizes with the host computer.

> *NOTE*   Checking this option automatically unchecks **Establish network connection** and **Launch application**. Similarly, checking either one of those options automatically unchecks **Launch ActiveSync**.

Establish Network Connection

Check this option to have iDockIt establish a connection to your network when you place the mobile computer in a serial or USB cradle or connect it to a serial or USB cable. In order to establish a connection to your network, you must connect the mobile computer to a host computer with a RAS server.

If you check this option, **Launch ActiveSync** is automatically unchecked.

You can check this option in conjunction with **Launch application**. After iDockIt establishes the network connection, it launches the specified application.

Launch Application

Check this option to have iDockIt launch the selected application when you place the mobile computer in a serial or USB cradle or connect it to a serial or USB cable. iDockIt uses the specified command line parameters. You must select an application to launch.

Select…

1.   Tap **Select** to open the **Select Auto-Launch Application** dialog.

2. Select a **File Type** in the drop-down list.

3. Select a Folder (as needed).

4. Select a file name in the list.

5. Use the input panel to specify command line parameters.

6. Tap **OK** at the top of the screen.

The selected application appears in the settings tab.

Serial Cradle Baud Rate

This option allows you to specify the baud rate iDockIt should use for a serial cable or cradle. Set this rate to match the host computer that the cradle or cable is connected to.

If you are using a USB cradle or cable, the USB driver automatically determines the connection speed.

Modem Cradle Settings

If you use a modem cradle, you can automatically connect to a remote host computer or network or you can synchronize with a host computer with which you have set up a partnership using ActiveSync. Alternatively, you can connect to your network and/or launch a specified application on the mobile computer.
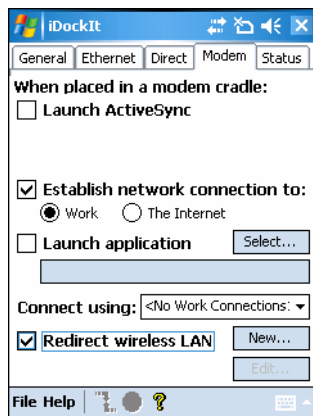
Figure B-6   *Modem Settings Tab*

Launch ActiveSync

Check this option to have iDockIt launch ActiveSync when you place the mobile computer in a modem cradle.

> ✓ **NOTE**   Checking this option automatically unchecks **Establish network connection** and **Launch application**. Similarly, checking either one of those options automatically unchecks **Launch ActiveSync**.

Establish Network Connection

Check this option to have iDockIt establish a network connection when you place the mobile computer in a modem cradle. iDockIt uses the modem connection specified in the **Connect using** list in this tab.

If you check this option, **Launch ActiveSync** is automatically unchecked.

You can check this option in conjunction with **Launch application**. After iDockIt establishes the network connection, it launches the specified application.

Launch Application

Check this option to have iDockIt launch the selected application when you place the mobile computer in a modem cradle. iDockIt uses the specified command line parameters. You must select an application to launch. If Establish network connection is checked, the application does not launch until a connection is successfully established.

Select...

1. Tap **Select** to open the **Select Auto-Launch Application** dialog.

2. Select a **File Type** in the drop-down list.

3. Select a Folder (as needed).

4. Use the input panel to specify command line parameters.

5. Select a file name in the list.

6. Tap **OK** at the top of the screen.

The selected application appears in the settings tab.

Choose Connection

The **Connect using** drop-down list includes all modem connections that you have defined for the mobile computer. Choose the one you wish to use.

If you check the General settings options to **Display settings when cradled** and **Auto-connect after x seconds**, you have an opportunity to select the appropriate modem connection when you cradle the mobile computer.

If you do not check the above options, iDockIt uses the last modem connection you selected.

Tap **New** to create a new modem connection.

Tap **Edit** to change the settings of an existing modem connection.

Tap **Delete** to delete the currently displayed modem connection.

Create A New Modem Connection

1. Get the following information from your ISP or network administrator: dial-up access telephone number, user name, password, domain name, and TCP/IP settings.

2. Tap **New** below the **Connect using** list.

3. Enter a name for the connection.

4. In the Modem list, tap your modem type. For the modem cradle, tap **Hayes Compatible on COM1**.

5. Tap **Configure** and change any Port Settings in the Connection Properties dialog, depending on requirements for your modem.

6. Tap **Next** after entering the connection name and choosing a modem.

7. Enter the access phone number and then tap **Next**.

8. Enter Login information (user name, password, and domain name) and then tap **Next**.

9. You should not need to change any TCP/IP settings unless directed by your ISP or network administrator. Tap **Next** and then tap **Finish** in the next server address dialog.

The new modem connection is in the drop-down list.

Edit an Existing Modem Connection

1. In the **Connect using** list, select the modem connection you need to modify.

2. Tap **Edit**.

3. In the **Connection Properties** dialog, make any necessary changes to the connection name, modem, or modem configuration options. Tap **Next** to continue or **OK** to close the dialog.

4. If you continue, you can change the access phone number. Tap **Next** to continue or **OK** to close the dialog.

5. If you continue, you can change your login information. If you need to make any TCP IP setting changes, tap **Next**. Otherwise, tap **OK** to close the dialog.

Delete an Existing Modem Connection

1. In the **Connect using** list, select the modem connection you want to delete.

2. Tap and hold the **Connect using** box until the pop-up menu displays.

3. Select **Delete** from the pop-up menu.

4. A dialog is displayed prompting you to conform that you want to delete the modem connection. Tap **Yes**.

The modem connection is removed from the drop-down list.

Configuring iDockIt for Windows CE 5.0

To run iDockIt, tap **Start** > **Programs** > **iDockIt**. When iDockIt is running, the icon ⬚ appears in the Task Tray. Tap the icon to display the iDockIt menu.
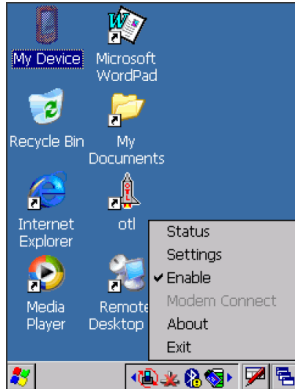
Figure B-7   *iDockIt Menu*

- **Status** displays the **Status** tab.

- **Settings** displays the **Settings** tab for the current connection or, if the mobile computer is not connected to a host computer via a cable or cradle, the most recently viewed settings tab.

- **Enable** is a toggle switch that checks/unchecks the **Enable iDockIt** setting on the **General** tab.

- **Modem Connect** is enabled when you have defined a modem connection in the modem settings tab. Tapping this item when the mobile computer is in the modem cradle initiates dial-out.

- **About** displays version and copyright information.

- **Exit** disables iDockIt and closes the application.

iDockIt includes five tab pages:

- **General** - General setup options for enabling/disabling iDockIt and displaying status and other information.

- **Ethernet** - Settings for what iDockIt should do when it detects that the mobile computer is in an Ethernet cradle.

- **Direct** - Settings for what iDockIt should do when it detects that the mobile computer is in a Serial or USB cradle or connected to a host computer using a Serial or USB cable.

- **Modem** - Settings for what iDockIt should do when it detects that the mobile computer is in a Modem cradle.

- **Status** - Current connection status, continuously updated, scrollable window.

Quick Start

Follow these guidelines. Refer to sections of this document devoted to individual tabs for details on settings and options

How To Prepare the Mobile Computer To Connect

Using Microsoft ActiveSync, ensure you have established a partnership between the mobile computer and the host computer. This should happen the first time you cradle the mobile computer. If you are using an Ethernet cradle, you must set up the partnership with the host computer using a serial or USB cable or cradle.

For more information, see ActiveSync Help on the host computer.

How To Start iDockIt

Tap **Start** > **Programs** > **iDockIt**. The **General** tab displays.

How to Enable iDockIt to Manage Connections

On the iDockIt **General** tab, check **Enable iDockIt**. iDockIt makes connections and carry out tasks according to the settings you have defined for each cradle type until you uncheck this option or exit.

To connect automatically to your host computer or network:

1.   Tap **Enable iDockIt** in the **General** tab.

2.   **Check or uncheck Display status when cradled**.

3.   Check **Display settings when cradled**. When you cradle the mobile computer, the **Settings** tab displays automatically.

4.   Uncheck the **Autoconnect** option.

5.   Tap the iDockIt tab that corresponds to your cradle type.

     a.   For an Ethernet cradle, check **Launch ActiveSync** and select the host computer you want to connect to.

     b.   For a direct connection using a USB cradle/cable, serial cable/cradle, or for a Modem cradle, check **Launch ActiveSync**; if you wish to connect to a host computer other than the one to which you are physically connected, check **Sync** with and choose the host computer in the list. (In ActiveSync Connections, select **Allow serial...connection** and **Allow network...connection**.)

     c.   To connect to a network using any type of cradle, tap **Establish network connection**.

To connect manually to your host computer or network:

While iDockIt is designed to connect the mobile computer to a specified host computer or network automatically, you can also choose your connection manually whenever you cradle the mobile computer.

1.   Tap **Enable iDockIt** in the **General** tab.

2.   **Check or uncheck Display status when cradled**.

3.   Check **Display settings when cradled**. When you cradle the mobile computer, the **Settings** tab displays automatically.

4.   Uncheck the **Autoconnect** option.

5.   Tap the iDockIt tab that corresponds to your cradle type.

6.   Check **Establish network connection** and optionally **Launch application**.

When you place the mobile computer in a cradle, iDockIt displays the **Settings** tab corresponding to that cradle. Choose the type of connection and tap . Another way to connect manually is to establish new connection settings before you cradle the mobile computer.

To launch an application when you connect:

1. Tap the iDockIt **General** tab.

2. Check **Enable iDockIt**.

3. Tap the tab that corresponds to the type of cradle you are using.

4. Tap **Launch Application**.

5. Tap **Select** and select the application you want to launch whenever the mobile computer is connected to a host computer or network. Enter any necessary program arguments.

6. Tap **OK**.

To determine the mobile computer's connection status:

Tap the iDockIt **Status** tab.

- **Dock Status** shows either **Docked** or **Not docked**.

- **Connection** shows either the name of the connection or **Not connected**.

- If the mobile computer is placed in the cradle, IP address shows all valid IP addresses assigned to the mobile computer. If the mobile computer is not in the cradle, IP address shows the IP address of your network adapter(s) or, if you do not have a network connection, a default address.

- The **Status** window shows all cradle events that have occurred since the last time you placed the mobile computer in the cradle.

Minimize iDockIt

To minimize iDockIt, tap **X** in the upper right corner of the screen. iDockIt controls cradle events while it is minimized.

Exit iDockIt

To close the application, tap **File** > **Exit**. iDockIt does not control cradle events when it is closed.

General Recommendations

The mobile computer should not be cradled or connected when the host computer to which it is physically connected is started or restarted. If the mobile computer is cradled when the host computer is started/restarted, the mobile computer attempts to connect before ActiveSync has fully loaded and a proper connection is impossible. Follow these general guidelines for avoiding connection problems:

- Connect only one mobile computer to the host computer at a time. (You can have more than one serial cable/cradle or USB cable/cradle connected simultaneously.)

- When you start or restart the host computer, wait for the start process to finish completely before cradling a mobile computer. When you cradle the mobile computer, it is able to make the connection defined in iDockIt settings.

- If the mobile computer was connected to the host computer when the host computer was started, remove the mobile computer from its cradle, restart the host computer, and then return the mobile computer to its cradle.

- Performing a soft reset on the mobile computer can be useful. Remove the mobile computer from its cradle before doing a soft reset. Restart iDockIt and then recradle the mobile computer.

- For additional information, refer to Microsoft ActiveSync Help on your host computer.

General Setup Options

Settings on the **General** tab complement the options you set for your cradle.
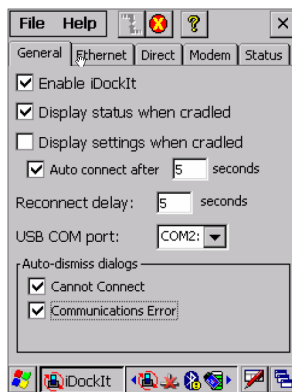
Figure B-8   *General Settings Tab*

Enable IDockIt

Check this option to enable iDockIt to control cradle events. When you cradle your handheld mobile computer, iDockIt identifies the type of cradle and perform the activities you have configured.

Uncheck this option to restore control of cradle events to Microsoft ActiveSync.

Display Status When Cradled

Check this option to display the iDockIt **Status** tab when you cradle the mobile computer. If you also checked **Display** settings when cradled, you first see the **Settings** tab for the type of cradle detected and then the **Status** tab after the specified time elapses.

Uncheck this option to prevent display of the iDockIt Status tab when you cradle the mobile computer.

Display Settings When Cradled

Check this option to display the cradle settings tab when you cradle the mobile computer. You can also check **Auto connect after x seconds** to have iDockIt wait a specified time before creating a connection. The delay gives you the opportunity to review/change cradle settings. During this waiting period, you can select either ![icon] or ![icon] in the menu bar to connect immediately or cancel automatic connection.

⚠ **WARNING!** **If you do not check this option (or if you check this option but do not specify the number of seconds), iDockIt displays the cradle settings tab when you cradle the mobile computer but does not attempt to establish a connection.**

Uncheck this option to prevent display of the cradle settings tab.

Reconnect Delay

This feature has not been implemented.

USB COM Port

The first time you run iDockIt, the application attempts to determine whether the mobile computer has a USB port and if so, the COM port to which it is mapped.

If iDockIt does not find a USB port, **None** display. You can then choose from all available COM ports in the list. In most cases, you should not have to change this setting.

Auto-dismiss Error Dialogs

You can configure iDockIt to dismiss several error dialogs that might display. To auto-dismiss an error message, tap the check box next to its title. If the message occurs during a connection attempt, iDockIt allows it on your behalf and the event appears in the Status window.

- **Port Disconnected**

  Cannot start communications with the desktop computer. The connection was terminated.

  What this message means: This message is displayed when you remove the mobile computer from a cradle, breaking the connection. Since this is not really an error, the message can be dismissed automatically.

- **Communications Error**

  Cannot start communications with the desktop computer. The computer is either not available or busy and currently cannot accept connections.

  What this message means: This message is displayed when ActiveSync attempts to connect to a host computer and synchronize data but cannot find the computer name. Since this message may appear in the course of a successful connection attempt, it can be dismissed automatically.

Status Tab

If iDockIt is enabled when you cradle the mobile computer, the Status tab displays connection-related events as they occur. Check **Display status when cradled** on the **General** tab if you want iDockIt to display this tab automatically whenever you cradle the mobile computer.
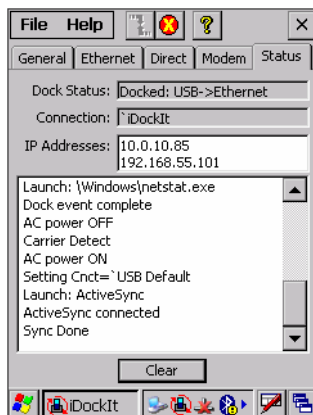
Figure B-9   *Status Tab*

The **Dock Status** field shows **Docked** and identifies the type of connection (Serial Direct, Modem, Ethernet, USB). The field shows **Not docked** when you remove the mobile computer from the cradle.

The **Connection** field shows either the name of your connection or Not connected.

The **IP addresses** field shows all valid IP addresses assigned to the mobile computer. When the mobile computer is not cradled, this field shows either the IP address of your network adapter or, if you do not have a network connection, a default IP address.

The **Status** window displays a scrolling list of cradle events as they occur, including:

- **AC power ON** and **OFF** as you cradle/uncradle the mobile computer.
- **Carrier detect**, baud rate, and **(cradle type) connect** when iDockIt identifies the cradle and connection speed.
- **Launch (application)** when iDockIt launches an application, followed by confirmation when the application has been launched successfully.
- **Sync done** when synchronization has completed successfully.
- **Dismiss (error message)** when iDockIt dismisses a message you have designated.
- **Dock event complete** when iDockIt has completed all defined tasks. If you uncradle the mobile computer before this item appears, regardless of dock status, you may interrupt assigned tasks.

Tap **Clear** to empty all events from the Status window.

Ethernet Cradle Settings

If you are using an Ethernet cradle, you can automatically connect to and sync with a partnered host computer on your network. Alternatively, you can establish a generic connection to your network and/or launch a specified application on the mobile computer.

> **NOTE**   You cannot use ActiveSync 4.0 or later to synchronize data between a host computer and a Windows CE-based device through an Ethernet cradle.
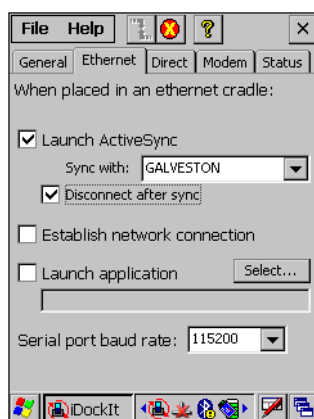
Figure B-10   *Ethernet Settings Tab*

Launch ActiveSync

Check this option to have iDockIt launch ActiveSync when you cradle the mobile computer. ActiveSync connects to the host computer specified in the **Sync with** option on your network.

> **NOTE**   Before you can select this option, you must connect to the host computer with a serial or USB cable or cradle and use ActiveSync to set up a partnership with that host computer.
>
> Checking this option automatically unchecks **Establish network connection** and **Launch application**. Similarly, checking either one of those options automatically unchecks **Launch ActiveSync**.

- **Sync with**

  Your handheld mobile computer can have partnerships with up to two host computers. This list shows only the host computers with which the mobile computer has a partnership. Select the host computer with which you want ActiveSync to sync data.

- **Disconnect after sync**

  Check this option to disconnect automatically from the selected host computer when ActiveSync has completed synchronization.

Establish Network Connection

Check this option to have iDockIt establish a connection to your network when you cradle the mobile computer.

If you check this option, **Launch ActiveSync** is automatically unchecked.

You can check this option in conjunction with **Launch application**. After iDockIt establishes the network connection, it launches the specified application.

Launch Application

Check this option to have iDockIt launch the selected application when you place the mobile computer in the cradle. iDockIt uses the specified command line parameters. You must select an application to launch.

If you check this option, **Launch ActiveSync** is automatically unchecked.

Select...

1. Tap the **Select** button to open the **Select Auto-Launch Application** dialog.

2. Select a **File Type** in the drop-down list.

3. Select a **Folder** (as needed).

4. Select a file name in the list.

5. Use the input panel to specify command line parameters.

6. Tap **OK** at the top of the screen.

The selected application appears in the settings tab.

Serial Port Baud Rate

This option allows you to specify the baud rate iDockIt should use for a serial connection to the Ethernet cradle. Set this rate to match the baud rate configured for the cradle. For maximum performance, always use the maximum baud rate of 115200.

If using a USB-to-Ethernet cradle, the USB driver automatically controls the connection speed.

Direct (Serial/USB) Settings

If you use a serial or USB cradle or connect to the mobile computer with a serial or USB cable, you can automatically connect to the connected host computer or network OR you can choose a host computer with which you have set up a partnership using ActiveSync. Alternatively, if your host computer supports RAS connections you can connect to your network through your host computer and/or launch a specified application on the mobile computer.
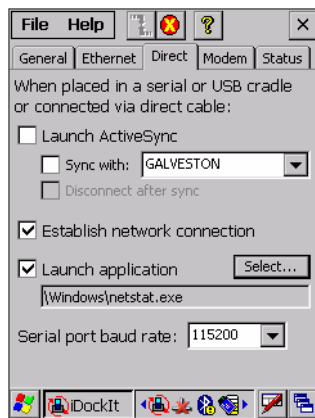
Figure B-11   *Direct (Serial/USB) Settings Tab*

Launch ActiveSync

Check this option to have iDockIt launch ActiveSync when you place the mobile computer in a serial or USB cradle or when you connect it to a serial or USB cable.

> **NOTE**   Checking this option automatically unchecks Establish network connection and Launch application. Similarly, checking either one of those options automatically unchecks Launch ActiveSync.

- **Sync with:**

  When this option is not checked, the mobile computer synchronizes data with the host computer to which it is connected. To synchronize with a different host computer, check this option and select the host computer in the list.

  ActiveSync is able to connect to this alternate host computer automatically ONLY IF you check this option.

- **Disconnect after sync** is available only if you select this option.

- **Disconnect after sync**

  Check this option to disconnect automatically from the host computer when ActiveSync has completed synchronization.

Establish Network Connection

Check this option to have iDockIt establish a connection to your network when you place the mobile computer in a serial or USB cradle or connect it to a serial or USB cable. In order to establish a connection to your network, you must connect the mobile computer to a host computer with a RAS server. If you have ActiveSync running on your host computer, it can be used as a RAS server.

If you check this option, **Launch ActiveSync** is automatically unchecked.

You can check this option in conjunction with **Launch application**. After iDockIt establishes the network connection, it launches the specified application.

Launch Application

Check this option to have iDockIt launch the selected application when you place the mobile computer in a serial or USB cradle or connect it to a serial or USB cable. iDockIt uses the specified command line parameters. You must select an application to launch.

Select…

1. Tap **Select** to open the **Select Auto-Launch Application** dialog.

2. Select a **File Type** in the drop-down list.

3. Select a **Folder** (as needed).

4. Select a file name in the list.

5. Use the input panel to specify command line parameters.

6. Tap **OK** at the top of the screen.

The selected application appears in the settings tab.

Serial Port Baud Rate

This option allows you to specify the baud rate iDockIt should use for a serial cable or cradle. Set this rate to match the host computer that the cradle or cable is connected to.

If you are using a USB cradle or cable, the USB driver automatically controls the connection speed.

USB Notes

The InVision USB cradle driver for the host computer maps the USB port to a virtual COM port, assigning it the next available port number. Refer to the user guide for your cradle.

Before you install the driver, open ActiveSync Connection Settings to see which ports are available. After you install the driver, a new COM port is available. Select this port for your USB cradle.

Check **Allow USB....** in ActiveSync Connection Settings only if you have a direct USB connection (no cradle) to the mobile computer.

If you restart your host computer or ActiveSync, the port selection may revert to COM1. Display Connection Settings and re-select the correct USB COM port.

Modem Cradle Settings

If you use a modem cradle, you can automatically connect to a remote host computer or network or you can choose a host computer with which you have set up a partnership using ActiveSync. Alternatively, you can connect to your network and/or launch a specified application on the mobile computer.
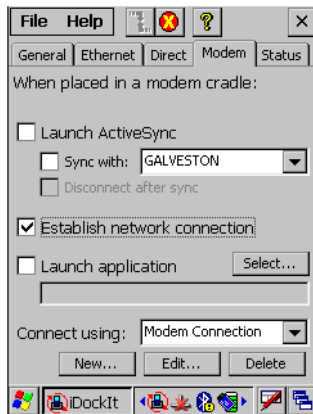
Figure B-12   *Modem Settings Tab*

Launch ActiveSync

Check this option to have iDockIt launch ActiveSync when you place the mobile computer in a modem cradle.

NOTE   Checking this option automatically unchecks **Establish network connection** and **Launch application**. Similarly, checking either one of those options automatically unchecks **Launch ActiveSync**.

- **Sync with:**

  When this option is not checked, the mobile computer synchronizes data with the host computer that is directly connected to the remote modem. To synchronize with a different host computer, check this option and select the host computer in the list.

  Disconnect after sync is available only if you select this option.

- **Disconnect after sync**

  Check this option to disconnect automatically from the selected host computer when ActiveSync has completed synchronization.

Establish Network Connection

Check this option to have iDockIt establish a network connection when you place the mobile computer in a modem cradle. iDockIt uses the modem connection specified in the **Connect using** list in this tab.

If you check this option, **Launch ActiveSync** is automatically unchecked.

You can check this option in conjunction with **Launch application**. After iDockIt establishes the network connection, it launches the specified application.

Launch Application

Check this option to have iDockIt launch the selected application when you place the mobile computer in a modem cradle. iDockIt uses the specified command line parameters. You must select an application to launch.

If **Establish network connection** is checked the application does not be launched until a connection is successfully established.

Select...

1.   Tap **Select** to open the **Select Auto-Launch Application** dialog.

2. Select a **File Type** in the drop-down list.

3. Select a **Folder** (as needed).

4. Use the input panel to specify command line parameters.

5. Select a file name in the list.

6. Tap **OK** at the top of the screen.

The selected application appears in the settings tab.

Choose Connection

The **Connect using** drop-down list includes all modem connections that you have defined for the mobile computer. Choose the one you wish to use.

If you check the General settings options to **Display settings when cradled** and **Auto-connect after x seconds**, you have an opportunity to select the appropriate modem connection when you place the mobile computer in the cradle.

If you do not check the above options, iDockIt uses the last modem connection you selected.

Tap **New** to create a new modem connection.

Tap **Edit** to change the settings of an existing modem connection.

Tap **Delete** to delete the currently displayed modem connection.

Create A New Modem Connection

1. Get the following information from your ISP or network administrator: dial-up access telephone number, user name, password, domain name, and TCP/IP settings.

2. Tap **New** below the **Connect using** list.

3. In the Connection Properties dialog, enter a name for the connection.

4. In the Modem list, tap your modem type. For the modem cradle, tap **Hayes Compatible on COM1**.

5. Tap **Configure** and change any Port Settings or Call Options in the Device Properties dialog, depending on requirements for your modem.

6. Tap **Next** after entering the connection name and choosing a modem.

7. Enter the access phone number and then tap **Next**.

8. Enter Login information (user name, password, and domain name) and then tap **Next**.

9. You should not need to change any TCP/IP settings unless directed by your ISP or network administrator. Tap **Next** and then tap **Finish** in the next server address dialog.

The new modem connection is in the drop-down list.

Edit An Existing Modem Connection

1. In the **Connect using** list, select the modem connection you need to modify.

2. Tap **Edit**.

3. In the Connection Properties dialog, make any necessary changes to the connection name, modem, or modem configuration options. Tap **Next** to continue or **OK** to close the dialog.

4. If you continue, you can change the access phone number. Tap **Next** to continue or **OK** to close the dialog.

5. If you continue, you can change your login information. If you need to make any TCP IP setting changes, tap **Next**. Otherwise, tap **OK** to close the dialog.

Delete An Existing Modem Connection

1. In the **Connect using** list, select the modem connection you want to delete.

2. Tap **Delete**.

3. The Modem Settings dialog asks you to confirm that you want to delete the named modem connection. Tap **Yes**.

The modem connection is removed from the drop-down list.

Un-installing iDockIt

For Windows Mobile 5.0 devices:

1. Exit iDockIt.

2. In the **System** tab, tap the **Remove Programs** icon.

3. Select **InVision iDockIt** in the program list.

4. Tap **Remove** and select **Yes** in the **Remove Program** dialog.

5. Tap **OK**.

For Windows CE 5.0 devices:

1. Exit iDockIt.

2. Tap **Start** > **Settings** and double-tap the **Remove Programs** icon.

3. Select **InVision iDockIt** in the program list.

4. Tap **Remove** and select **Yes** in the **Remove Program** dialog.

5. Ignore the **Remove Programs Error** dialog if it appears. Tap **OK**.

6. Close the **Remove Programs** dialog and **Settings** windows.

Glossary

Numeric

802.11. A group of wireless specifications developed by the Institute of Electrical and Electronics Engineers (IEEE). It specifies an over-the-air interface between a wireless client and a base station or between two wireless clients.

802.11a. Operates in the 5 GHz frequency range (5.125 to 5.85 GHz) with a maximum 54Mbit/sec. signaling rate. The 5 GHz frequency band is not as crowded as the 2.4 GHz frequency because it offers significantly more radio channels than the 802.11b and is used by fewer applications. It has a shorter range than 802.11g and is not compatible with 802.11b.

802.11b. Operates in the 2.4 GHz Industrial, Scientific and Measurement (ISM) band (2.4 to 2.4835 GHz) and provides signaling rates of up to 11Mbit/sec. This is a very commonly used frequency. Microwave ovens, cordless phones, medical and scientific equipment, as well as Bluetooth devices, all work within the 2.4 GHz ISM band.

802.11g. Similar to 802.11b, but this standard supports signaling rates of up to 54Mbit/sec. It also operates in the heavily used 2.4 GHz ISM band but uses a different radio technology to boost overall throughput. Compatible with the 802.11b.

A

Access Point. Provides a bridge between Ethernet wired LANs and the wireless network. Access points are the connectivity point between Ethernet wired networks and devices (laptops, hand-held computers, point-of-sale terminals) equipped with a wireless LAN adapter card.

Ad Hoc Mode. A wireless network framework in which devices communicate directly with one another without using an access point.

API. An interface by means of which one software component communicates with or controls another. Usually used to refer to services provided by one software component to another, usually via software interrupts or function calls

Application Programming Interface. See **API**.

ANSI Terminal. A display terminal that follows commands in the ANSI standard terminal language. For example, it uses escape sequences to control the cursor, clear the screen and set colors. Communications programs support the ANSI terminal mode and often default to this terminal emulation for dial-up connections to online services.

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.

Association. The process of determining the viability of the wireless connection and establishing a wireless network's root and designated access points. A mobile computer associates with its wireless network as soon as it is powered on or moves into range.

Autodiscrimination. The ability of an interface controller to determine the code type of a scanned bar code. After this determination is made, the information content is decoded.

B

Bar. 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.

Bluetooth. A low-cost, short-range radio link between two devices. Bluetooth can replace cables and can be used to create ad hoc networks and provide a standard way to connect devices.

Bit. Binary digit. One bit is the basic unit of binary information. Generally, eight consecutive bits compose one byte of data. The pattern of 0 and 1 values within the byte determines its meaning.

bps. See **Bits Per Second**.

Byte. On an addressable boundary, eight adjacent binary digits (0 and 1) combined in a pattern to represent a specific character or numeric value. Bits are numbered from the right, 0 through 7, with bit 0 the low-order bit. One byte in memory is used to store one ASCII character.

BOOTP. A protocol for remote booting of diskless devices. Assigns an IP address to a machine and may specify a boot file. The client sends a bootp request as a broadcast to the bootp server port (67) and the bootp server responds using the bootp client port (68). The bootp server must have a table of all devices, associated MAC addresses and IP addresses.

boot or boot-up. The process a computer goes through when it starts. During boot-up, the computer can run self-diagnostic tests and configure hardware and software.

C

CAM. (Continuously Aware Mode) Mode in which the adapter is instructed to continually check for network activity.

CDMA. (Code Division Multiple Access) A digital cellular technology that uses spread spectrum techniques that separates them through the use of digital frequency codes across the full available spectrum.

CDRH. (Center for Devices and Radiological Health) A federal agency responsible for regulating laser product safety. This agency specifies various laser operation classes based on power output during operation.

CDRH Class 1. This is the lowest power CDRH laser classification. This class is considered intrinsically safe, even if all laser output were directed into the eye's pupil. There are no special operating procedures for this class.

CDRH Class 2. No additional software mechanisms are needed to conform to this limit. Laser operation in this class poses no danger for unintentional direct human exposure.

CHAP. (Challenge Handshake Authentication Protocol) A type of authentication in which the authentication agent (typically a network server) sends the client program a random value that is used only once and an ID value. Both the sender and peer share a predefined secret. The peer concatenates the random value (or nonce), the ID and the secret and calculates a one-way hash using MD5. The hash value is sent to the authenticator, which in turn builds that same string on its side, calculates the MD5 sum itself and compares the result with the value received from the peer. If the values match, the peer is authenticated.

Character. A pattern of bars and spaces which either directly represents data or indicates a control function, such as a number, letter, punctuation mark, or communications control contained in a message.

Character Set. Those characters available for encoding in a particular bar code symbology.

Check Digit. A digit used to verify a correct symbol decode. The scanner inserts the decoded data into an arithmetic formula and checks that the resulting number matches the encoded check digit. Check digits are required for UPC but are optional for other symbologies. Using check digits decreases the chance of substitution errors when a symbol is decoded.

Codabar. A discrete self-checking code with a character set consisting of digits 0 to 9 and six additional characters: (-$:/,+).

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 (space, minus (-), plus (+), period (.), dollar sign ($), slash (/), and percent (%)). 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

Data Communications Equipment (DCE). A device (such as a modem) which is designed to attach directly to a DTE (Data Terminal Equipment) device.

DCE. See **Data Communications Equipment**.

DCP. See **Device Configuration Package**.

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.

Device Configuration Package. The Symbol Device Configuration Package provides flash partitions, Terminal Configuration Manager (TCM) and the associated TCM scripts. With this package hex images that represent flash partitions can be created and downloaded to the mobile computer.

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.

DRAM. Dynamic random access memory.

DTE. See **Data Terminal Equipment**.

E

EAN. (European Article Number) This European/International version of the UPC provides its own coding format and symbology standards. Element dimensions are specified metrically. EAN is used primarily in retail.

EAP. (Extensible Authentication Protocol) A general authentication protocol used to control network access. Many specific authentication methods work within this framework.

EAP-PEAP. (Extensible Authentication Protocol-Protected Extensible Authentication Protocol) A mutual authentication method that uses a combination of digital certificates and another system, such as passwords.

EAP-TLS. (Extensible Authentication Protocol-Transport Layer Security) A mutual authentication method that uses digital certificates.

EDGE. (Enhanced Data rates for GSM Evolution) Allows wireless transmission of data at speeds up to 384K bps. It's based on GSM technology and allows for high-bandwidth services such as multimedia.

Element. Generic term for a bar or space.

Encoded Area. Total linear dimension occupied by all characters of a code pattern, including start/stop characters and data.

Encryption. Encoding data to prevent it from being read by unauthorized people.

ENQ (RS-232). ENQ software handshaking is also supported for the data sent to the host.

Ethernet . An IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium.

ESD. Electro-Static Discharge

F

Flash Disk. An additional megabyte of non-volatile memory for storing application and configuration files.

Flash Memory. Flash memory is nonvolatile, semi-permanent storage that can be electronically erased in the circuit and reprogrammed.

File Transfer Protocol (FTP). A TCP/IP application protocol governing file transfer via network or telephone lines. See **TCP/IP.**

FTP. See **File Transfer Protocol**.

G

GPS. (Global Positioning System) A "constellation" of 24 satellites that orbit the Earth at a height of 10,900 miles, making it possible for people using ground receivers to determine their geographic location within 10 to 100 meters. The satellites

use simple mathematical calculations to broadcast information that is translated as longitude, latitude and altitude by Earth-based receivers.

GPRS. (General Packet Radio Service) A technology that runs at speeds up to 115Kbit/sec., compared with the 9.6Kbit/sec. of older GSM systems. It enables high-speed wireless Internet and other communications such as e-mail, games and applications. It supports a wide range of bandwidths and is an efficient use of limited bandwidth. It's particularly suited for sending and receiving small amounts of data, such as e-mail and Web browsing, as well as large volumes of data.

GSM. (Global System for Mobile Communications) A digital cellular system based on TDMA narrowband technology, which gives users access to time slots on the same frequency bands. It allows up to eight simultaneous communications on the same frequency.

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.

IEEE Address. See **MAC Address**.

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.

IOCTL. Input/Output Control.

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**.

I/O Ports. interface The connection between two devices, defined by common physical characteristics, signal characteristics, and signal meanings. Types of interfaces include RS-232 and PCMCIA.

Input/Output Ports. I/O ports are primarily dedicated to passing information into or out of the terminal's memory. Series 9000 mobile computers include Serial and USB ports.

IP. (Internet Protocol) The IP part of the TCP/IP communications protocol. IP implements the network layer (layer 3) of the protocol, which contains a network address and is used to route a message to a different network or subnetwork. IP accepts "packets" from the layer 4 transport protocol (TCP or UDP), adds its own header to it and delivers a "datagram" to the layer 2 data link protocol. It may also break the packet into fragments to support the maximum transmission unit (MTU) of the network.

IP Address. (Internet Protocol address) The address of a computer attached to an IP network. Every client and server station must have a unique IP address. A 32-bit address used by a computer on a IP network. Client workstations have either a permanent address or one that is dynamically assigned to them each session. IP addresses are written as four sets of numbers separated by periods; for example, 204.171.64.2.

IPX/SPX. Internet Package Exchange/Sequential Packet Exchange. A communications protocol for Novell. IPX is Novell's Layer 3 protocol, similar to XNS and IP, and used in NetWare networks. SPX is Novell's version of the Xerox SPP protocol.

IS-95. Interim Standard 95. The EIA/TIA standard that governs the operation of CDMA cellular service. Versions include IS-95A and IS-95B. See CDMA.

K

Key. A key is the specific code used by the algorithm to encrypt or decrypt the data. Also see, **Encryption** and **Decrypting**.

L

laser scanner. A type of bar code reader that uses a beam of laser light.

LASER. (Light Amplification by Stimulated Emission of Radiation) The laser is an intense light source. Light from a laser is all the same frequency, unlike the output of an incandescent bulb. Laser light is typically coherent and has a high energy density.

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.

LCD. See **Liquid Crystal Display**.

LEAP. (Lightweight Extensible Authentication Protocol) A mutual authentication method that uses a username and password system.

LED Indicator. A semiconductor diode (LED - Light Emitting Diode) used as an indicator, often in digital displays. The semiconductor uses applied voltage to produce light of a certain frequency determined by the semiconductor's particular chemical composition.

Liquid Crystal Display (LCD). A display that uses liquid crystal sealed between two glass plates. The crystals are excited by precise electrical charges, causing them to reflect light outside according to their bias. They use little electricity and react relatively quickly. They require external light to reflect their information to the user.

Light Emitting Diode. See **LED**.

M

MC. Mobile computer.

MDN. (Mobile Directory Number) The directory listing telephone number that is dialed (generally using POTS) to reach a mobile unit. The MDN is usually associated with a MIN in a cellular telephone -- in the US and Canada, the MDN and MIN are the same value for voice cellular users. International roaming considerations often result in the MDN being different from the MIN.

MIL. 1 mil = 1 thousandth of an inch.

MIN. (Mobile Identification Number) The unique account number associated with a cellular device. It is broadcast by the cellular device when accessing the cellular system.

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 Symbol Series 9090 wireless portable computer. It can be set up to run as a stand-alone device, or it can be set up to communicate with a network, using wireless radio technology.

MS CHAP. (Microsoft Challenge Handshake Authentication Protocol) is the Microsoft version of CHAP and is an extension to RFC 1994. Like the standard version of CHAP, MS-CHAP is used for PPP authentication; in this case, authentication occurs between a PC using Microsoft Windows NT or Microsoft Windows 95 and a Cisco router or access server acting as a network access server (NAS).

N

Nominal. The exact (or ideal) intended value for a specified parameter. Tolerances are specified as positive and negative deviations from this value.

Nominal Size. Standard size for a bar code symbol. Most UPC/EAN codes are used over a range of magnifications (e.g., from 0.80 to 2.00 of nominal).

NVM. Non-Volatile Memory.

O

ODI. See **Open Data-Link Interface**.

Open Data-Link Interface (ODI). Novell's driver specification for an interface between network hardware and higher-level protocols. It supports multiple protocols on a single NIC (Network Interface Controller). It is capable of understanding and translating any network information or request sent by any other ODI-compatible protocol into something a NetWare client can understand and process.

Open System Authentication. Open System authentication is a null authentication algorithm.

P

PAN . Personal area network. Using Bluetooth wireless technology, PANs enable devices to communicate wirelessly. Generally, a wireless PAN consists of a dynamic group of less than 255 devices that communicate within about a 33-foot range. Only devices within this limited area typically participate in the network.

Parameter. A variable that can have different values assigned to it.

PC Card. A plug-in expansion card for laptop computers and other devices, also called a PCMCIA card. PC Cards are 85.6mm long x 54 mm wide, and have a 68 pin connector. There are several different kinds:
Type I; 3.3 mm high; use - RAM or Flash RAM
Type II; 5 mm high; use - modems, LAN adaptors
Type III; 10.5 high; use - Hard Disks

PCMCIA. Personal Computer Memory Card Interface Association. See **PC Card**.

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%.

PING. (Packet Internet Groper) An Internet utility used to determine whether a particular IP address is online. It is used to test and debug a network by sending out a packet and waiting for a response.

Print Contrast Signal (PCS). Measurement of the contrast (brightness difference) between the bars and spaces of a symbol. A minimum PCS value is needed for a bar code symbol to be scannable. PCS = (RL - RD) / RL, where RL is the reflectance factor of the background and RD the reflectance factor of the dark bars.

Programming Mode. The state in which a scanner is configured for parameter values. See **Scanning Mode**.

Q

Quiet Zone. A clear space, containing no dark marks, which precedes the start character of a bar code symbol and follows the stop character.

QWERTY. A standard keyboard commonly used on North American and some European PC keyboards. "QWERTY" refers to the arrangement of keys on the left side of the third row of keys.

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.

Router. A device that connects networks and supports the required protocols for packet filtering. Routers are typically used to extend the range of cabling and to organize the topology of a network into subnets. See **Subnet**.

RS-232. An Electronic Industries Association (EIA) standard that defines the connector, connector pins, and signals used to transfer data serially from one device to another.

S

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

Secure Sockets Layer (SSL). SSL is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL is included as part of both the Microsoft and Netscape browsers and most Web server products. Developed by Netscape, SSL also gained the support of Microsoft and other Internet client/server developers as well and became the de facto standard until evolving into Transport Layer Security. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

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.

SHIP. Symbol Host Interface Program.

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.

SMDK. Symbol Mobility Developer's Kit.

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

TCP/IP. (Transmission Control Protocol/Internet Protocol) A communications protocol used to internetwork dissimilar systems. This standard is the protocol of the Internet and has become the global standard for communications. TCP provides transport functions, which ensures that the total amount of bytes sent is received correctly at the other end. UDP is an alternate transport that does not guarantee delivery. It is widely used for real-time voice and video transmissions where erroneous packets are not retransmitted. IP provides the routing mechanism. TCP/IP is a routable protocol, which means that all messages contain not only the address of the destination station, but the address of a destination network. This allows TCP/IP messages to be sent to multiple networks within an organization or around the

world, hence its use in the worldwide Internet. Every client and server in a TCP/IP network requires an IP address, which is either permanently assigned or dynamically assigned at startup.

Telnet. A terminal emulation protocol commonly used on the Internet and TCP/IP-based networks. It allows a user at a terminal or computer to log onto a remote device and run a program.

Terminate and Stay Resident (TSR). A program under DOS that ends its foreground execution to remain resident in memory to service hardware/software interrupts, providing background operation. It remains in memory and may provide services on behalf of other DOS programs.

Terminal Emulation. A "terminal emulation" emulates a character-based mainframe session on a remote non-mainframe terminal, including all display features, commands and function keys. The MC909X Series supports Terminal Emulations in 3270, 5250 and VT220.

TFTP. (Trivial File Transfer Protocol) A version of the TCP/IP FTP (File Transfer Protocol) protocol that has no directory or password capability. It is the protocol used for upgrading firmware, downloading software and remote booting of diskless devices.

TKIP. (Temporal Key Integrity Protocol) A wireless encryption protocol that periodically changes the encryption key, making it harder to decode.

Tolerance. Allowable deviation from the nominal bar or space width.

Transmission Control Protocol/Internet Protocol. See **TCP/IP.**

TLS. (Transport Layer Security) TLS is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

Trivial File Transfer Protocol. See **TFTP.**

TSR. See **Terminate and Stay Resident**.

U

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.

UDP. (User Datagram Protocol) A protocol within the IP protocol suite that is used in place of TCP when a reliable delivery is not required. For example, UDP is used for real-time audio and video traffic where lost packets are simply ignored, because there is no time to retransmit. If UDP is used and a reliable delivery is required, packet sequence checking and error notification must be written into the applications.

U

Visible Laser Diode (VLD). A solid state device which produces visible laser light.

W

Warm Boot. A warm boot restarts the mobile computer by closing all running programs. All data that is not saved to flash memory is lost.

WAP. (Wireless Application Protocol) A set of specifications, developed by the WAP Forum, that lets developers using Wireless Markup Language build networked applications designed for handheld wireless devices. WAP was designed to work within the constraints of these devices: a limited memory and CPU size, small, monochrome screens, low bandwidth and erratic connections.

WEP. Wired-Equivalent Privacy protocol was specified in the IEEE 802.11 standard to provide a WLAN with a minimal level of security and privacy comparable to a typical wired LAN, using data encryption.

WPA. Wi-Fi Protected Access is a data encryption specification for 802.11 wireless networks that replaces the weaker WEP. It improves on WEP by using dynamic keys, Extensible Authentication Protocol to secure network access, and an encryption method called Temporal Key Integrity Protocol (TKIP) to secure data transmissions.

WPA2. Wi-Fi Protected Access 2 is an enhanced version of WPA. It uses Advanced Encryption Standard instead of TKIP.

WLAN. Wireless local-area networks use radio waves instead of a cable to connect a user device, such as a mobile computer, to a LAN. They provide Ethernet connections over the air and operate under the 802.11 family of specifications developed by the IEEE.

Index

MOTOROLA

72E-72216-06 Revision A - December 2007