Dolphin® 7900 Mobile Computer

Windows Mobile™ 2003 Second Edition Software for Pocket PCs

User's Guide - Prelim. Draft Rev (a)

powered by
Adaptus™
imaging technology

Disclaimer

Hand Held Products, Inc. d/b/a HHP (“HHP”) reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult HHP to determine whether any such changes have been made. The information in this publication does not represent a commitment on the part of HHP.

HHP shall not be liable for technical or editorial errors or omissions contained herein; nor for incidental or consequential damages resulting from the furnishing, performance, or use of this material.

Web Address: www.hhp.com

Trademarks

Dolphin, HomeBase, Mobile Base, and QuadCharger are trademarks or registered trademarks of Hand Held Products, Inc.

Windows Mobile, Windows, Windows NT, Windows 2000, Windows ME, Windows XP, ActiveSync, Outlook, and the Windows logo are trademarks or registered trademarks of Microsoft Corporation.

Intel is a registered trademark of Intel Corporation.

Chapter 9 (pages 9-1–9-11) contains copyrighted information from SyChip, Inc.

Chapter 9 (pages 9-12–9-25) contains copyrighted information from Meetinghouse Corporation. Meetinghouse, the Meetinghouse logo, and all other Meetinghouse trademarks/service marks contained herein are trademarks or registered trademarks of Meetinghouse.

Chapter 10 is copyrighted information used by permission from Bluetooth SIG, Inc.
The Bluetooth trademarks are owned by Bluetooth SIG, Inc., U.S.A. and licensed to HHP.

Chapter 11 (11-3–11-15 and 11-17–11-22) contains information with permission from INTRINSYC Software, Inc.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Table of Contents

Chapter 1 - Introduction

Chapter 2 - Getting Started

Chapter 3 - Dolphin 7900 Hardware Overview

Chapter 4 - Using the Dolphin 7900

Chapter 5 - Using the Image Engine

Chapter 6 - Using Dolphin 7900 Keyboards

Chapter 7 - Settings

Chapter 8 - Communications

Chapter 9 - Wireless LAN Communications with 802.11b

Chapter 10 - Wireless PAN Communications with Bluetooth

Chapter 11 - Wireless WAN Communications with GSM/GPRS

Chapter 13 - Dolphin 7900 HomeBase

Chapter 14 - Dolphin 7900 Mobile Base

Chapter 15 - Dolphin 7900 ChargeBase

Chapter 16 - Dolphin 7900 QuadCharger

Chapter 17 - Warranty, Service, and Support

1 Introduction

Congratulations on the purchase of the Dolphin 7900 mobile computer! You have made a wise choice in selecting the Dolphin, a device known worldwide for its ergonomic form factor, light-weight, rugged design and single-handed data collection capabilities.

Ergonomics

The patented shape of the Dolphin 7900 fits into either hand comfortably with major function keys that are easy to access. The adjustable hand strap on the back panel ensures a secure grip on the terminal for solid one-handed operation in mobile environments.

Rugged Design

Dolphin 7900 terminals are the most durable mobile computers on the market. Their rugged design can withstand repeated five-foot drops onto a concrete floor, extreme temperatures, as well as high humidity, moisture, and dust conditions. The terminals are independently tested to meet IP64 specifications.

Mobile Computing Features

- A low-power, high-resolution digital image engine for omni-directional and auto-discrimination decoding of most bar code symbologies; see Bar Code Symbologies Supported on page 5-1.
- Wireless Full Area Networking™ (WFAN) technology supports integrated LAN, PAN, and WAN wireless networks
- An Intel® X-Scale 400MHz RISC microprocessor for fast processing
- Microsoft Windows Mobile 2003 Second Edition Software for Pocket PCs
- 64 MB RAM and 64 MB synchronous Flash memory configuration for ample and secure data storage
- A mini-Secure Digital (SD) memory interface that enables memory expansion

Additional Features

- Long-lasting Lithium Ion (Li-ion) batteries
- 3.8”, easy-to-read 1/4 VGA (240 x 320) backlit TFT color display with touch screen
- Two keyboard options: 25-key numeric-alpha, and 36-key full alpha-numeric
- Industrial-grade mechanical connector that supports serial and USB communications, as well as power in and out
- Full suite of compatible peripheral devices
- Decoding of stacked linear and matrix codes with Optical Character Recognition (OCR) functionality
- Scan button on both side panels for fast, easy one-hand scanning with either hand
- Digital picture capability
- Audio jack for headset use
- Speaker and microphone on the front panel

Application Development Tools

- HHP Dolphin SDK Add-on for Pocket PC 2003 - supports Embedded Visual C++ 4.0
- HHP Dolphin .NET SDK for Pocket PC 2002 and 2003 - supports Visual Studio.NET 2003 (VB.NET and C#.NET)
- HHP Dolphin GSM/GPRS SDK Add-on for Pocket PC 2003 - supports Embedded Visual C++ 4.0 and Visual Studio.NET 2003

This User’s Guide

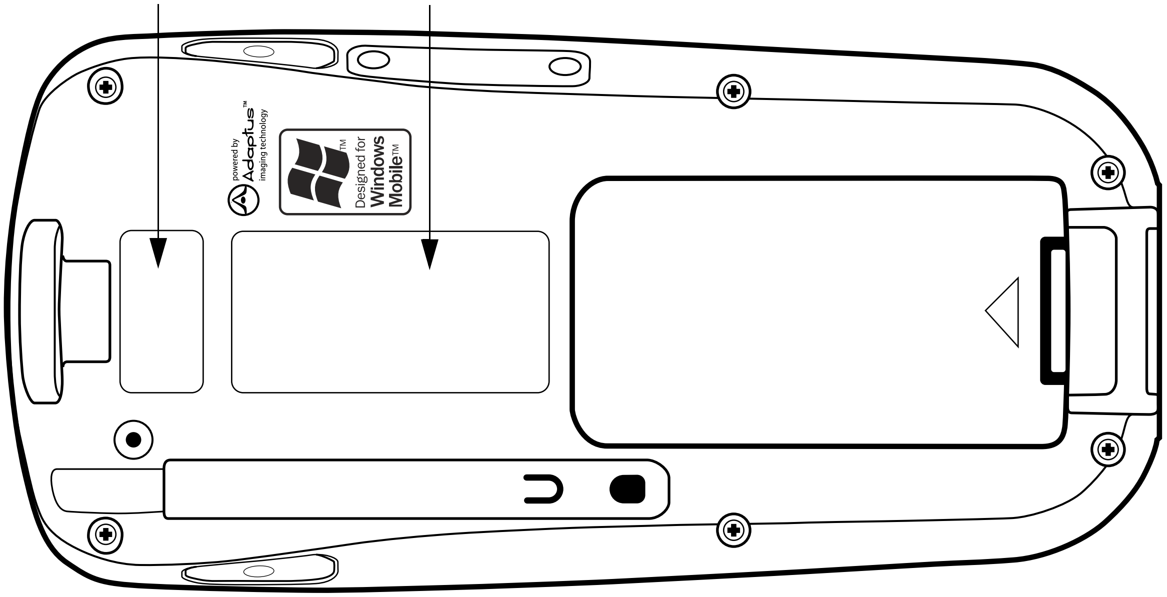
The Dolphin 7900 Mobile Computer User’s Guide provides you with the information you need to make the most of your Dolphin terminal.

Required Safety Labels

Dolphin 7900 mobile computers meet or exceed the requirements of all applicable standards organizations for safe operation. However, as with any electrical equipment, the best way to ensure safe operation is to operate them according to the agency guidelines that follow. Please read these guidelines carefully before using your Dolphin mobile computer.

Location

Safety labels appear in these locations.



Regulatory and Safety Approvals for all Dolphin 7900 Terminals

Parameter	Specification
U.S.A	FCC Part 15, Class B
Canada	ICES-003
European Community	EN 55022 (CISPR 22) Class B
	EN60950
	EN60825-1
	EN55024:1998

The CE Mark on the product indicates that the system has been tested to and conforms with the provisions noted within the 89/336/EEC Electromagnetic Compatibility Directive and the 73/23/EEC Low Voltage Directive.

For further information, please contact:

Hand Held Products, Inc.
Nijverheidsweg 9
5627 BT Eindhoven
The Netherlands

HHP shall not be liable for use of our product with equipment (i.e., power supplies, personal computers, etc.) that is not CE marked and does not comply with the Low Voltage Directive.

Dolphin 7900 WLAN or WPAN Radio

Dolphin 7900 RF terminals are designed to comply with the most current applicable standards on safe levels of RF energy developed by the Institute of Electrical and Electronics Engineers (IEEE) and the American National Standards Institute (ANSI) and has been recommended for adoption by the Federal Communications Commission (FCC).

802.11b

The following is the required safety label that appears on the back panel of Dolphin 7900 terminals equipped with an 802.11b radio:

Bluetooth

The following is the required safety label that appears on the back panel of Dolphin 7900 terminals equipped with a Bluetooth radio:

802.11b and Bluetooth

The following is the required safety label that appears on the back panel of the Dolphin 7900 terminals equipped with an 802.11b and a Bluetooth radio combination:

Dolphin 7900 WWAN Radio

Dolphin 7900 RF terminals are designed to comply with the most current applicable standards on safe levels of RF energy developed by the Institute of Electrical and Electronics Engineers (IEEE) and the American National Standards Institute (ANSI) and has been recommended for adoption by the Federal Communications Commission (FCC).

GSM

The following is the required safety label that appears on the back panel of Dolphin 7900 terminals equipped with a GSM radio:

GSM and 802.11b

The following is the required safety label that appears on the back panel of Dolphin 7900 terminals equipped with a GSM and 802.11b radio combination:

GSM and Bluetooth

The following is the required safety label that appears on the back panel of Dolphin 7900 terminals equipped with a GSM and Bluetooth radio combination:

GSM, Bluetooth, and 802.11b

The following is the required safety label that appears on the back panel of Dolphin 7900 terminals equipped with a GSM, Bluetooth, and 802.11b radio combination:

FCC Compliance

Dolphin mobile computers meet or exceed all applicable standards and have been manufactured to the highest level of quality.

Dolphin 7900 Batch Terminal

Dolphin 7900 Batch terminals comply with part 15 of the FCC rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Dolphin 7900 RF Terminal with 802.11b, Bluetooth, and/or GSM Radios

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

If necessary, the user should consult the dealer or an experienced radio/television technician for additional suggestions. The user may find the following booklet helpful: “Something About Interference.” This is available at FCC local regional offices. Our company is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by our company. The correction is the responsibility of the user. Use only shielded data cables with this system.

In accordance with FCC 15.21, changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

⚠ **This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter. To maintain compliance with FCC RF exposure guidelines for body-worn operation, do not use accessories that contain metallic components and ensure that the antenna is at least 15mm (0.6 inches) from the body.**

Canadian Compliance

This Class B digital apparatus complies with Canadian ICES-003. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing.

Cet appareil numérique de la Classe B est conforme à la norme NMB-003 du Canada.

RF, Regulatory, and Safety Agency Approvals for 802.11b and Bluetooth

Parameter	Specification
RF Approvals	
U.S.A	FCC Part 15.247
Canada	RSS 210

RF, Regulatory, and Safety Agency Approvals for GSM

Parameter	Specification
RF Approvals	
U.S.A	FCC Part 24
Canada	RSS 133

Dolphin 7900 802.11b and/or Bluetooth R&TTE Compliance Statement

Dolphin 7900 RF terminals are in conformity with all essential requirements of the R&TTE Directive (1999/5/EC). This equipment has been assessed to the following standards:

Parameter	Specification
R&TTE	EN 300 328-2:2000 EN 301 489-1 (2002-08) EN 301 489-17 (2002-08) EN 60950:2000 EN 50361:2001

This product is marked with CE0681 (!) in accordance with the Class II product requirements specified in the R&TTE Directive, 1999/5/EC.

The equipment is intended for use throughout the European Community. Its authorization for use in France is restricted as follows:

PAN European Frequency Range: 2.402 - 2.480 GHz

Restrictions in France are as follows:

- Indoor use - Maximum power (EIRP*) of 100 mW for the entire 2400-2483.5 MHz
- Outdoor use - Maximum power (EIRP*) of 100 mW for the 2400-2454 MHz band and maximum power (EIRP*) of 10 mW for the 2454-2483 MHz band.

Dolphin 7900 GSM R&TTE Compliance Statement

Dolphin 7900 terminals are in conformity with all essential requirements of the R&TTE Directive (1999/5/EC). This equipment has been assessed to the following standards:

Parameter	Specification
R&TTE	EN 301 511: 2000 EN 301 489-1 (2002-08) EN 301 489-7 (2002-08) EN 60950:2000 EN 50361:2001

Pacemakers, Hearing Aids and Other Electrically Powered Devices

Most manufacturers of medical devices adhere to the IEC 601-1-2 standard. This standard requires devices to operate properly in an EM Field with a strength of 3V/m over a frequency range of 26 to 1000MHz.

The maximum allowable field strength emitted by the Dolphin is 0.3V/m according to Subpart B of Part 1 of the FCC rules. Therefore, the Dolphin RF has no effect on medical devices that meet the IEC specification.

Microwaves

The radio in the Dolphin RF terminal operates on the same frequency band as a microwave oven. Therefore, if you use a microwave within range of the Dolphin RF terminal you may notice performance degradation in your wireless network. However, both your microwave and your wireless network will continue to function.

The Dolphin Batch terminal does not contain a radio, and therefore, is not affected by microwave ovens.

Care and Cleaning of the Dolphin 7900

When needed, clean the image engine window and the LCD display with a clean, non-abrasive, lint-free cloth. The terminal can be cleaned with a damp cloth.

2

Getting Started

Overview

The Dolphin 7900 combines the latest in multi-functional wireless data and voice communications technology with a unique, compact form factor, which makes it an ideal solution for today’s in-transit applications.

Data Input

The Dolphin 7900 mobile computer features a PDA design with a larger display and smaller recessed keyboards. The display area is 3.8 inches with a 240 X 320 VGA display in TFT color that is backlit for maximum viewability, then covered with an industrial touch screen for maximum durability. There are two keyboard options - 25-key numeric-alpha and 36-key alpha-numeric.

Imaging

The Dolphin 7900 contains an integrated imager that can take digital images of damaged packages and recipient signatures in addition to decoding standard 1D and 2D symbologies. For the greatest ease-of-use when operating the imager, **both** side panels feature a scan button that initiates a scan with the touch of a thumb or forefinger.

Memory

The Dolphin 7900 is a Windows Mobile computer with 64 MB RAM and 64 MB non-volatile synchronous Flash memory.

Communications

Communications via the industrial, mechanical connector supports 115 Kbps using serial RS-232 and 12 Mbps using USB.

The Dolphin 7900 Series

The Dolphin 7900 terminal comprises one element of an enterprise data collection system that includes various models, peripherals, and accessories that you can combine to suit your exact needs.

Dolphin 7900 Models

Dolphin 7900 terminals are available in numerous radio configurations.

Dolphin 7900 WLAN (802.11b)

These terminals integrate the basic functionality of the Batch terminals with an integrated, IEEE 802.11b direct sequence radio that enable communication with a host computer through a wireless local area network (WLAN).

Dolphin 7900 WPAN (Bluetooth)

This terminal allows Bluetooth communications to Bluetooth enabled devices such as printers, mobile phones, access points, Bluetooth-enabled PCs, etc.

Dolphin 7900 WWAN (GSM/GPRS)

This terminal features all the benefits of the Dolphin 7900 with the additional capabilities of GSM/GPRS technology.

Dolphin 7900 WLAN and WPAN (802.11b and Bluetooth)

This terminal features co-located 802.11b and Bluetooth radios, which means that your terminal contains the capabilities of both radios. You can operate the radios simultaneously or switch between them.

Dolphin 7900 WWAN and WLAN (GSM/GPRS and 802.11b)

This terminal features the functionality of both GSM/GPRS and 802.11b radio and network technologies.

Dolphin 7900 WWAN and WPAN (GSM/GPRS and Bluetooth)

This terminal features the functionality of both GSM/GPRS and Bluetooth radio and network technologies.

Dolphin 7900 WWAN, WLAN, and WPAN (GSM/GPRS, 802.11b, and Bluetooth)

This terminal features the functionality of GSM/GPRS, 802.11b, and Bluetooth radio and network technologies.

Dolphin 7900 Peripherals

Each of the following items is sold separately to enhance your Dolphin 7900 terminal’s capabilities.

Dolphin HomeBase™

The Dolphin HomeBase charging and communication cradle supports both RS-232 and USB communications, which enable it to interface with the majority of PC-based enterprise systems. When a terminal is seated in the HomeBase, its main battery pack charges in less that four hours. In addition, the HomeBase contains an auxiliary battery well that charges a spare Li-ion battery.

For more information, see Dolphin 7900 HomeBase on page 13-1.

Dolphin Mobile Base

The Dolphin Mobile Base charging and communication cradle is designed specifically for in-premise and in-transit data collection applications. It features a flexible mounting bracket, a cigarette lighter adapter or power cable to adapt it to your environment.

When a terminal is seated in the Mobile Base, its main battery pack charges in less that four hours. The serial connector supports RS-232 communication and power out to peripheral devices, such as hand held scanners.

For more information, see Dolphin 7900 Mobile Base on page 14-1.

Dolphin ChargeBase

The Dolphin ChargeBase is a four-slot charging cradle that holds, powers, and charges a terminal in each slot.

For more information, see Dolphin 7900 ChargeBase on page 15-1.

Dolphin Net Base

The Dolphin Net Base is a four-slot charging/communication cradle that holds, powers, charges, and communicates with the terminal in each slot. Ethernet communication occurs via statically and dynamically-assigned IP addresses.

For more information about the Dolphin Net Base, please consult the Dolphin 7900 Net Base Quick Start Guide.

Dolphin QuadCharger™

The Dolphin QuadCharger is a four-slot charging station for Dolphin Li-ion battery packs that can charge each battery in less than four hours. The fourth slot features a battery analyzer that completely resets and re-calibrates a battery, then displays remaining capacity.

For more information, see Dolphin 7900 QuadCharger on page 16-1.

Dolphin 7900 Accessories

Each of the following items is sold separately to enhance your Dolphin 7900 terminal’s capabilities.

Charging/Communication Cables

USB and serial cables connect the Dolphin 7900 terminal directly to both a peripheral device for communication and a power source for charging.

Dolphin Mobile Charger

This charging cable plugs the terminal directly into a vehicle cigarette lighter/power port to power the terminal and charge the battery pack. This accessory converts the 12 Volts out of the vehicle to the 9 Volts required by the terminal.

Protective Enclosure

This enclosure wraps around the terminal to protect it from wear and tear.

Protective Holster

The protective holster secures the terminal for mobile use.

Dolphin Mobile Mount

The Dolphin Mobile Mount solution secures Dolphin 7900 in the cab of any vehicle. Used in conjunction with the Mobile Charger, Dolphin terminals can be adapted to almost any in-transit environment.

Li-ion Battery Pack

The 7.4v, 14.8 watt hour Li-ion rechargeable battery pack provides the main power supply for Dolphin 7900 terminals.

Using the Dolphin 7900 for the First Time

Step 1. Unpack the Carton and Verify its Contents

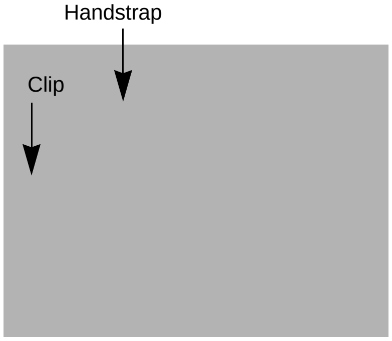
Verify that the carton contains the following items:

- Dolphin 7900 mobile computer (the terminal)
- Main battery pack (7.4v Li-ion)
- Microsoft Companion CD
- Dolphin 7900 Quick Start Guide

Be sure to keep the original packaging in the event that the Dolphin terminal should need to be returned for service. For details, see Return Information on page 17-2.

Each order includes a Dolphin Software Development Kit and User’s Guide CD; verify that you received this CD with your order. If you ordered accessories for your terminals, verify that they are also included with the order.

The Dolphin 7900 Handstrap



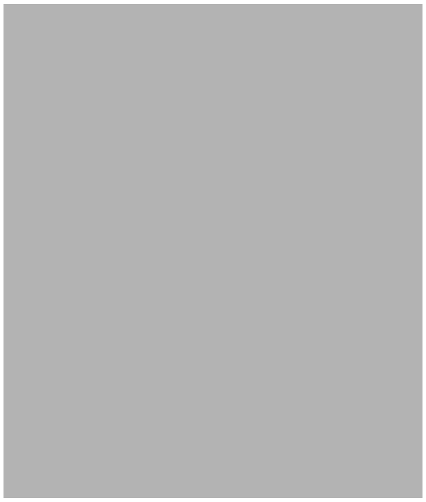
The Dolphin 7900 ships with the handstrap installed and fastened with a clip on the top panel. To install the battery pack, you must detach the handstrap.

1. Push the clip of the handstrap down and away from the terminal.
2. Move the strap up and away from the top panel.

Note: To re-attach the handstrap, slide the clip back into place on the top panel.

Step 2. Install the Main Battery Pack

Use only the Li-ion battery packs provided by HHP. The use of any battery pack not sold/manufactured by HHP in a Dolphin terminal will void your warranty and may result in damage to the Dolphin terminal or battery.



1. Unpack the Li-ion battery pack.
2. Hold the terminal with the front panel (keyboard) facing down and detach the handstrap.
3. Take the battery and insert the end without the locking tab into the top of the battery well and push down with a hinging motion until the locking tab snaps.
4. Re-attach the handstrap.

To Remove the Main Battery Pack

1. Detach the handstrap.
2. Press the locking tab on the battery pack away from the bottom panel.
3. Pull the battery pack up with a hinging motion.

Step 3. Charge the Main and Backup Batteries

The power supply for the Dolphin mobile computer consists of two types of battery power: the main battery pack installed on the back panel and the backup battery that resides inside the terminal.

The main battery powers the terminal. The internal backup battery charges off the main battery and maintains the application data stored in RAM and the system clock for up to 30 minutes when the terminal's main battery pack is completely discharged or removed.

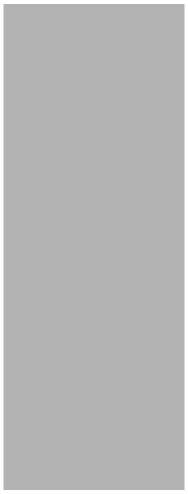
Before initial use - Because the terminals are shipped with both batteries discharged of all power, charge the main battery pack for a minimum of four hours before initial use.

When installed in the terminal, the battery pack can be charged in the HomeBase, Mobile Base, or with the appropriate charging cable. When not installed in the terminal, battery packs can be charged in the QuadCharger or the auxiliary well of the HomeBase.

Time to Charge - Four hours for the main battery pack, eight hours for the internal backup battery the first time.

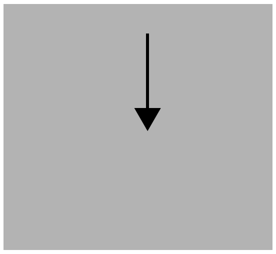
⚠ *Use only Dolphin 7900 series peripherals, power cables, and power adapters. Use of peripherals, cables, or power adapters not sold/manufactured by HHP will void the warranty and may damage the terminal.*

Using the Dolphin HomeBase



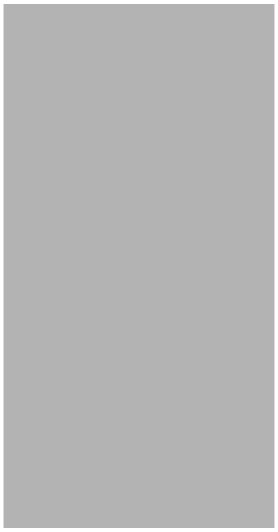
1. Connect the HomeBase to the power supply provided by HHP.
2. Slide the terminal (with installed battery pack) into the terminal well until the Dock LED lights solid green to indicate that the terminal is properly seated.
3. The battery pack begins charging.

Charging a Spare Battery Pack



The HomeBase features an auxiliary battery well. Insert a spare battery pack into this well and the battery charges in four hours. The auxiliary battery well charges batteries independently of the terminal well.

Using the Mobile Base



1. Connect the Mobile Base to the appropriate power source using an HHP cable.
2. Slide the terminal (with installed battery pack) into the terminal well until the Dock LED lights solid green to indicate that the terminal is properly seated.
3. The battery pack begins charging.

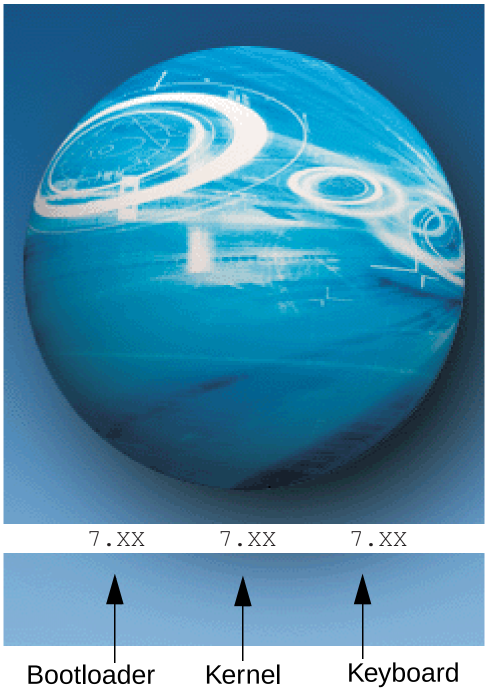
Other Charging Options

When the Li-ion battery is installed in the terminal, connect a charging and/or communication cable, such as the Mobile Charger, to the mechanical connector and plug the cable into a power outlet.

When the Li-ion battery is not installed in the terminal, place the battery pack in the Dolphin QuadCharger.

Step 4. Initialize the Mobile Computer

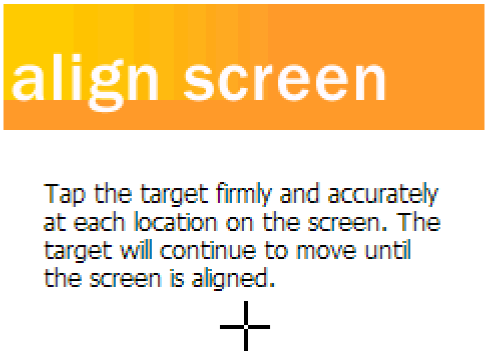
1. Power on the terminal. The decode LED lights and the scan LED blinks for approximately three seconds. Do **NOT** press any keys while the terminal is booting up.
2. The terminal initializes and the HHP splash screen displays for a few seconds. The Build numbers indicate the software version numbers.



3. The system performs a hard reset. When the display activates again, follow the instructions that appear.

Step 5. Align the Screen

You are prompted to align the screen by tapping the target five times. Use the stylus provided by HHP.



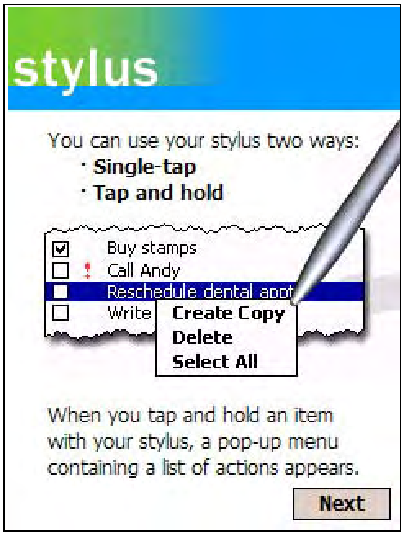
align screen

Tap the target firmly and accurately at each location on the screen. The target will continue to move until the screen is aligned.

- Alignment should always be performed with a stylus designed for touch screen applications. The small point is required for accurate calibration.
- Press the stylus firmly into the center of the cross-hair target once and release. Do not “double-tap” the target.
- You can re-align the screen at any time by going to **Start** > **Settings** > **System** tab > **Screen**.

Step 6. Complete the Screens

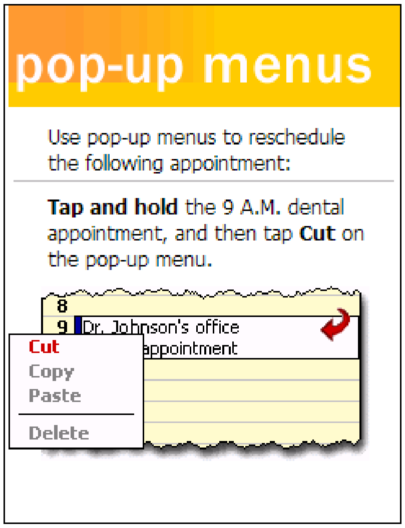
After aligning the screen, follow the directions on the screen which take you through a simple exercise showing how to use the stylus and pop-up menus.



stylus

You can use your stylus two ways:
- **Single-tap**
- **Tap and hold**

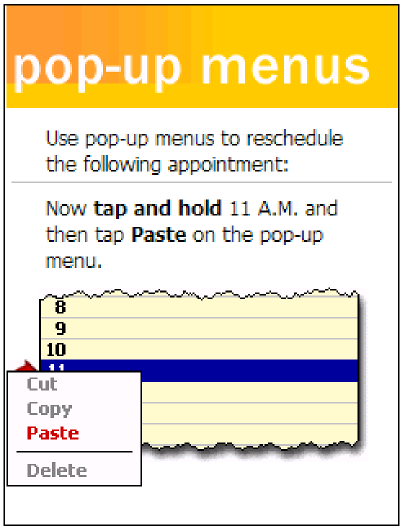
When you tap and hold an item with your stylus, a pop-up menu containing a list of actions appears.



pop-up menus

Use pop-up menus to reschedule the following appointment:

Tap and hold the 9 A.M. dental appointment, and then tap **Cut** on the pop-up menu.



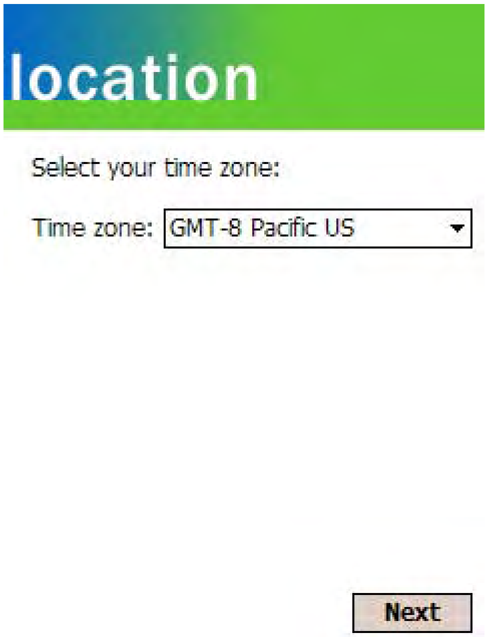
pop-up menus

Use pop-up menus to reschedule the following appointment:

Now **tap and hold** 11 A.M. and then tap **Paste** on the pop-up menu.

Note: HHP recommends using screen protectors for Dolphin 7900 terminals; especially for those terminals used within applications that require high-volume interaction with the touch screen. Screen protectors help prevent damage to the touch screen, are easily installed, and can be purchased at any major computer retail store or directly from HHP, Inc. Please contact HHP directly for part numbers and pricing.

Step 7. Set the Time Zone



location

Select your time zone:

Time zone: GMT-8 Pacific US

Use the drop-down list to select your time zone, and tap **Next**. This does not necessarily set the correct time; only the time zone. You set the time and date manually. For details, see Setting the Time and Date on page 2-9.

After setting the time zone, you are finished with the initial setup. The system begins autoinstalling.

Step 8. Autoinstall

For each program that loads, a status bar indicates that the program is loading. Autoinstall occurs after each hard reset. Do NOT touch the keyboard or the screen while programs are loading.

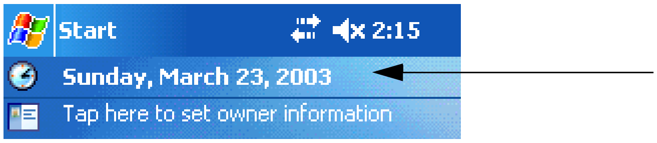
All configurations of the Dolphin 7900 terminal install HHP Demos and HHP Utilities. If the terminal is configured with a wireless radio, the appropriate radio drivers and utilities for each radio install.

After Autoinstall is complete, the terminal performs a soft reset automatically. When it finishes booting up after the soft reset, the Today screen appears; see Today Screen on page 4-2.

Setting the Time and Date

You need to re-set the time and date after every hard reset of the terminal. It is a good idea to set the time and date now before you begin using the device.

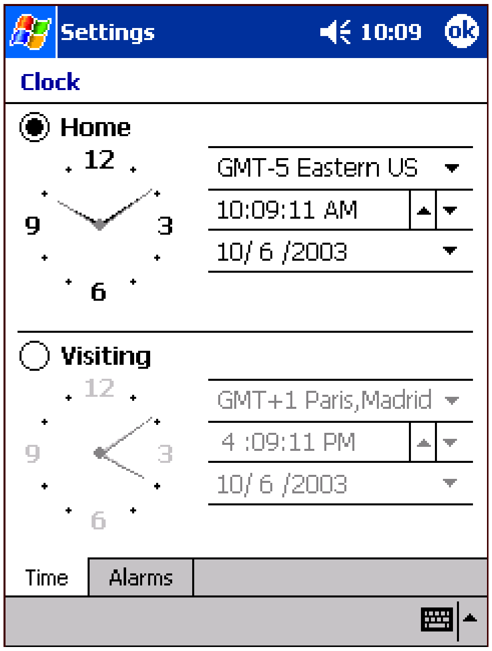
On the Today screen, tap the line that displays the time and date,



Sunday, March 23, 2003

Tap here to set owner information

The Clock Settings screen appears.



● Home

GMT-5 Eastern US

10:09:11 AM

10/ 6 /2003

○ Visiting

GMT+1 Paris,Madrid

4 :09:11 PM

10/ 6 /2003

Step 9. Verifying Operations with HHP Demos

The Dolphin 7900 mobile computer comes loaded with HHP Demos you can use to verify imaging and decoding.

Verify Imaging

The Image Demo enables you to use the imager to capture an image.

1. Go to **Start** > **HHP Demos** > **Image Demo**. The image demo opens.
2. Point the terminal at an object and press the SCAN key on the keyboard or the Scan button on the side panel.
   A preview of the object appears on the terminal screen.
3. Release the SCAN key. The image is captured. By default, the image saves to the My Device folder as “imagedemo.jpg.” To save to a different location, go to **File** > **Save As** and select a new location.
4. Press the ESC key to close the demo.

For more information about taking an image, see Using the Image Engine on page 5-1.

Verify Decoding

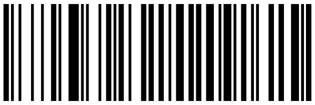
The Scan Demo enables you to decode a sample bar code.

1. Go to **Start** > **HHP Demos** > **Scan Demo**.
2. Aim the terminal at a bar code and press the SCAN key on the keyboard or the Scan button on the side panel.
   The scan LED lights red, and a green aimer beam projects out from the scanner.
3. When a good scan is obtained, the decode LED lights solid green and the terminal beeps.
   The bar code readout appears on the screen.
4. Press the ESC key to close the demo.

Sample Bar Codes

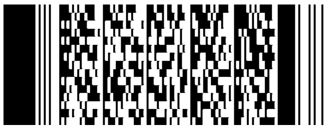
You can use the following bar codes to verify decoding:

Sample 128



Code 128

Sample PDF417



PDF417 Test Message

For more information, see Decoding on page 5-3.

Resetting the Terminal

There are two ways to reset the terminal: a soft and a hard reset.

Soft Reset (Warm Boot)

A soft reset re-boots the device without losing RAM data. You would perform a soft reset when

- the terminal fails to respond.
- after installing some software applications.
- after making changes to certain system settings, such as network cards.

1. Press and hold the Red + ESC keys for approximately five seconds.
2. The decode and scan LEDs flash for approximately three seconds as the terminal resets.
3. When the reset is complete, the Today screen displays.

Hard Reset (Cold Boot)

A hard reset resets the operating system, restores the terminal back to factory defaults, and resets the terminal after a bootloader, keyboard, and kernel upgrade.

⚠ *A hard reset erases all of the data stored in RAM memory and all RAM installed applications.*

1. Press and hold the Red + TAB keys for approximately five seconds.
2. The decode and scan LEDs light for approximately three seconds.
3. The terminal re-initializes; see Initialize the Mobile Computer on page 2-7.

Suspend Mode

To put the Dolphin terminal into suspend mode manually, press and hold the POWER key. The terminal goes into suspend mode automatically when the terminal is inactive for a programmed period of time. For more information, see Power on page 7-11.

To wake the Dolphin terminal from suspend mode, press the SCAN key.

The Dolphin terminal also goes into suspend mode if you remove the main battery pack while the terminal is powered on. After you install a new battery, press the SCAN key to wake the terminal.

⚠ *If the main battery and back-up battery are ever fully discharged of power, the terminal performs a hard reset when power is restored. The terminal will be restored to its original state. All data stored in RAM memory will be lost.*

3

Dolphin 7900 Hardware Overview

System Features

Processor

The Dolphin 7900 terminal is equipped with an Intel X-Scale 400MHz RISC microprocessor that runs on a 100 MHz RAM BUS, making it one of the most powerful mobile computers on the market.

Operating System

Windows Mobile 2003 Second Edition software provides a compact, highly efficient, scalable operating system. Its open architecture facilitates the development of applications for energy-efficient data collection devices such as the Dolphin 7900 terminal.

Memory

Main Board/IPSM – The standard memory configuration is 64 MB RAM and 64 MB non-volatile synchronous Flash.

Mini Secure Digital Card (SD) – Dolphin 7900 terminals contain a mini-SD memory interface to support memory expansion. You can order memory upgrades up to 128 MB or 256 MB. The SD access door on the left, side panel makes the SD memory user-accessible. However, when that access door is fastened securely and properly, the terminal’s environmental rating is preserved.

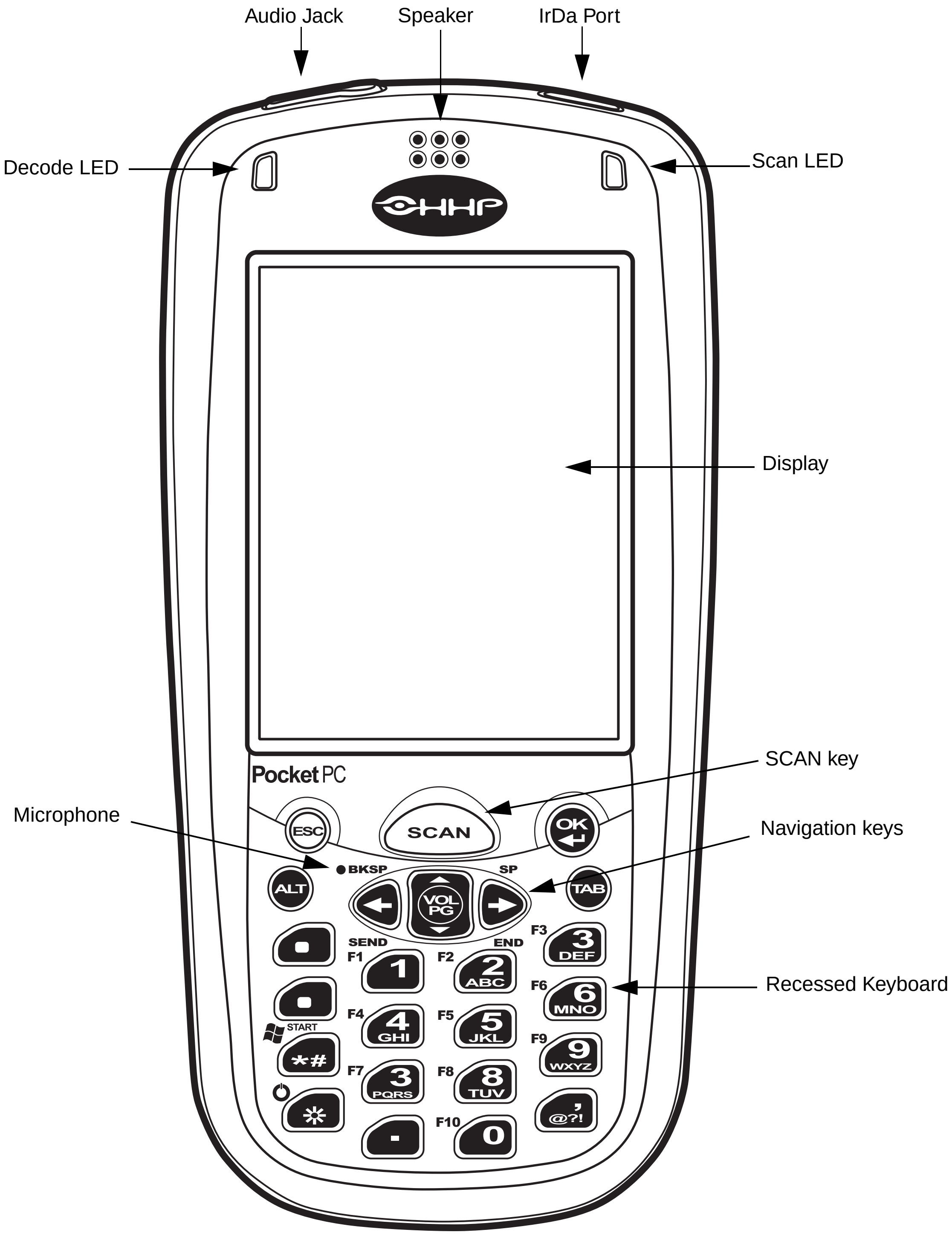
For more information about each kind of memory, see Memory on page 7-8.

Wireless Radio Options

For more information, see Radio Options on page 4-8.

Front Panel Features

This section describes features on the front panel of the Dolphin 7900 terminal. (The following graphic shows a Dolphin 7900 with a 25-key keyboard.)



Audio Jack

Dolphin 7900 terminals contain a 2.5mm audio jack supports both speaker (stereo) and microphone (mono) headsets. Microphone is available only on Dolphin 7900 terminals configured with GSM/GPRS radios. In both cases, you must use a 2.5mm plug. For more information about GSM/GPRS radios, see Wireless WAN Communications with GSM/GPRS on page 11-1.

Speaker

The Dolphin 7900 terminal has an integrated speaker that sounds audio signals as you scan bar code labels and enter data. The operating frequency range is 500Hz at 71 dB up to 80 dB. The speaker can also be used for playing sounds (e.g., WAV or MP3 files).

When used in conjunction with the microphone on the keyboard, the speaker can also be used for two-way voice communications. Both speaker and microphone are located on the front panel for voice communication that is fully integrated with terminal operation.

IrDA Port

The Infrared Data Association or IrDA port communicates with IrDA-enabled devices such as PC’s, printers, modems, or other Dolphin 7900 terminals. The maximum speed is 115kbps.

LEDs

The two light emitting diodes (LEDs) located at the top of the LCD display flash and illuminate during resets and scanning/imaging. Both can be programmed by various software applications.

Scan LED - Located in the upper right corner, this LED lights red when you press the SCAN key.
Decode LED - Located in the upper left corner, this LED lights green when a scanned bar code is successfully decoded.

Display

Dolphin 7900 terminals feature a 3.8” liquid crystal display (LCD) that is covered with an industrial, protective touch screen lens. The video graphic array (VGA) resolution is 1/4 (240 X 320 pixel). The touch screen is activated with the stylus (included with the terminal) or a finger.

The color LCD is 16 bits/pixel and uses active display or thin film transistor (TFT) technology. The backlight for the display illuminates when the screen is touched.

For more information about the Backlight, see Adjusting the Backlight on page 4-6.

SCAN Key

The SCAN key is centrally located for easy access with the right or left hand. When pressed, the SCAN key activates the scanner/imager. The SCAN key also functions as an on or system wakeup control for the terminal.

Navigation Keys

The centrally-located navigation keys enable you to move and position the cursor through software programs. The up and down arrows are programmed to perform specific functions when pressed in combination with the Blue and Red modifier keys.

Keyboard

The Dolphin 7900 series features two keyboard options: 25-key numeric-alpha and 36-key full alpha/numeric keyboard. Both keyboards are recessed under the overlay for maximum durability and backlit for easy viewing in various lighting conditions. Keyboard overlays are color-coded to indicate the functions performed or characters typed when the color-coded key is pressed immediately after the Red or Blue Modifier key.

For a complete overview of each keyboard, see Using Dolphin 7900 Keyboards on page 6-1.

Microphone

Dolphin 7900 terminals feature an integrated microphone that provides audio input to the terminal. Both microphone and speaker are located on the front panel for voice communication that is fully integrated with terminal operation.

Back Panel Features

The following graphic describes features on the back panel of the Dolphin 7900 terminal.

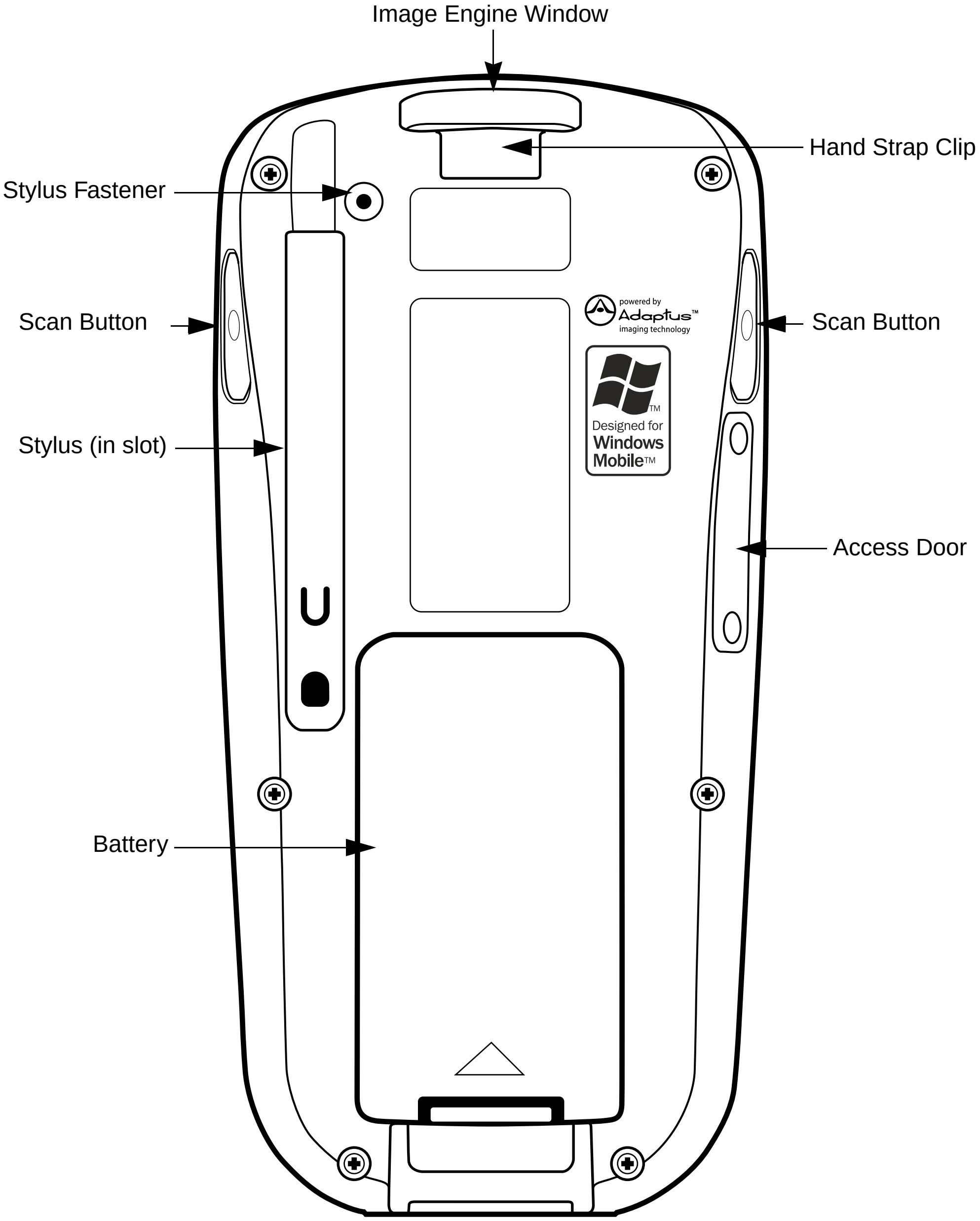


Image Engine Window

Dolphin 7900 terminals have an optional image engine that reads and decodes linear, stacked linear (PDF417), and 2D matrix bar code symbologies. With the latest CMOS-based technology, the engine works like a digital camera and enables digital image capture, signature capture, and reading of OCR characters.

The engine points out the top panel at a slight downward angle so that the terminal needs to be positioned slightly above the image or bar code when using the engine.

Hand Strap Clip

The Dolphin 7900 has an adjustable, elastic hand strap attached to the terminal with a clip on the top of the back panel. You can detach the handstrap from this clip when you need access to the battery or other item on the back panel.

Scan Button

See Scan Button on page 3-6.

Access Door

See Access Door on page 3-6.

Battery

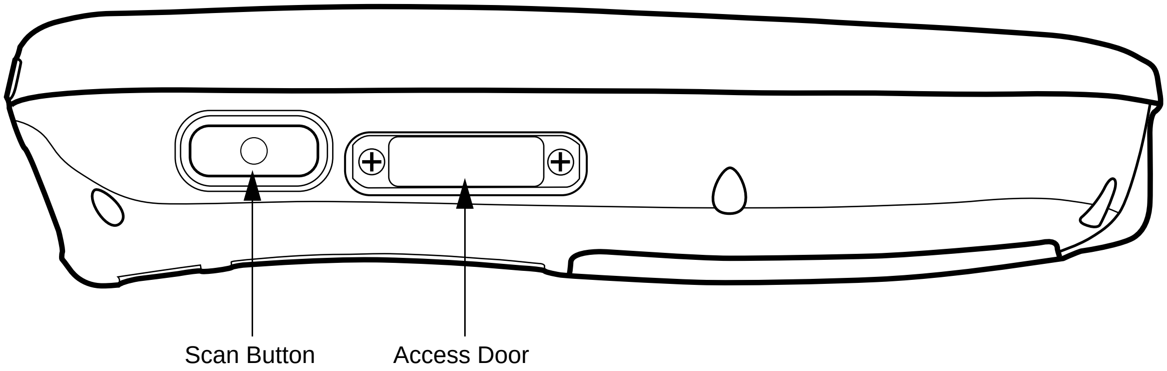
The Battery well is a recessed area on the back of the Dolphin that holds the Li-Ion battery pack.
For more information, see Battery Power on page 3-8.

Stylus and Fastener

The stylus is used to operate the touch screen. The back panel features this storage slot to hold the stylus when not in use. There is also a fastener on the back panel to which you can attach stylus tethers. A stylus tether is a coiled elastic cord with one end to attach to the stylus and another to attach fasten to the back panel.

Side Panel Features

The following graphic shows the left, side panel.

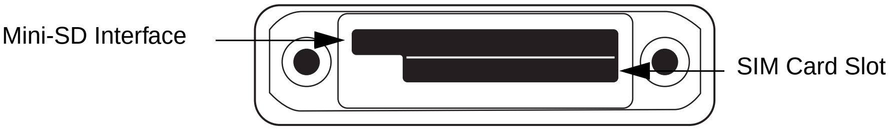


Scan Button

Scan buttons are located on both side panels. The Scan buttons initiate the image engine and can serve as a more ergonomic alternative to pressing the Scan key on the keyboard.

Access Door

When open, the access door on the Dolphin 7900 contains the mini-SD memory interface and the SIM card slot.



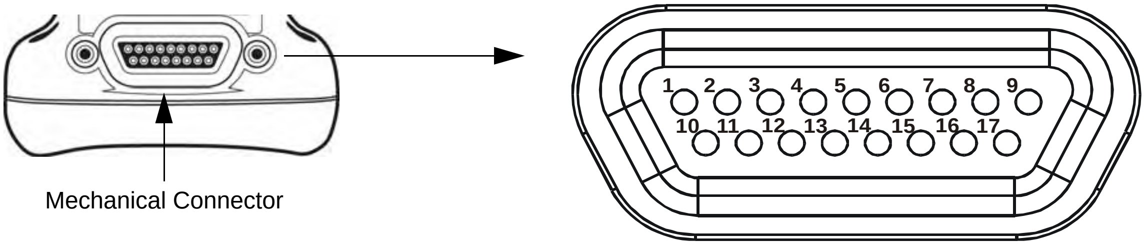
Mini-SD Interface	You can install a mini-SD card to expand the terminal's memory capacity up to 128MB or 256MB. After memory expansion is complete, this door should be closed and sealed. (The mini-SD memory interface does not support SDIO.)
SIM Card	SIM cards are required when using a GSM radio. For more information about GSM and SIM cards, see SIM Card Installation on page 11-2.

When closed, the access door seals the memory interface and SIM card from moisture and particle intrusion providing secure storage for read/write data.

Note: This door is not removable by the user in the field. The door can only be removed using a special Torx T8 tool from HHP. This tool is HHP part number 100001024.

Bottom Panel Features

This following graphics describe the bottom panel of the Dolphin 7900.



Pin #	Description
1	+USB
2	PWR
3	N / C
4	N / C
5	N / C
6	N / C
7	GND
8	5V OUT
9	DTR
10	-USB
11	USB DET
12	RI
13	DSR
14	RXD
15	RTS
16	TXD
17	CTS

Note: Signals referenced are for a DTE device.

Mechanical Connector

The bottom panel of the Dolphin 7900 features a custom, industrial-grade connector with 17 pins. When seated in a Dolphin 7900 series peripheral, the terminal is powered, the main battery charged, and communication occurs via this connector. All Dolphin 7900 series peripherals are designed to work exclusively with this connector.

The 17-pin connector can communicate with Dolphin 7900 series peripherals via RS-232 or USB. For RS-232, the maximum communication speed is 115 Kbps with seven baud rate settings. For USB, the communication speed is up to 12 Mbps. If the peripheral unit is connected to a PC, this connector also transmits data.

The mechanical connector also provides power out (to peripheral devices) 5V at 500mA. This means that, with the proper HHP cable, the terminal can power another device.

Battery Power

The Dolphin 7900 features intelligent battery technology with two types of battery power: the main battery pack installed in the back panel and the backup battery located inside the terminal. Both batteries work together to prevent data loss when the terminal is used over long periods of time. Both batteries must also be charged to full capacity before using the Dolphin 7900 for the first time.

Main Battery Pack

⚠ *Use only the Li-ion battery packs provided by HHP. The use of any battery pack not sold/manufactured by HHP in a Dolphin terminal will void your warranty and may result in damage to the Dolphin terminal or battery.*

The 7.4V, 14.8 watt hour Li-Ion battery pack is the primary power source for the Dolphin. The Li-Ion battery is designed to operate in a temperature range of -10 to 50° C (14 to 122° F). For the location of the Li-Ion battery on the terminal, see Battery on page 3-5.

Charging Options

When the Li-ion battery is installed in the terminal:

- Place the terminal in a HomeBase (page 13-7) or Mobile Base (page 14-4) that is connected to an appropriate power supply.
- Connect a charging/communication cable to the mechanical connector, plug the cable into the AC adapter, and plug the adapter cable into a power outlet.
- Connect the terminal to the Mobile Charger and vehicle power port.

When the Li-ion battery is not installed in the terminal:

- Place the battery pack in the Dolphin QuadCharger - see Charging Batteries in the QuadCharger on page 16-3.
- Place the battery pack in the auxiliary battery well of the HomeBase - see page 13-7.

Charging Time

The Li-ion battery pack requires four hours to charge to full capacity.

Internal Backup Battery

Located inside the terminal, the backup battery is a 3.6 Volt nickel metal hydride (NiMH) battery.

Purpose

The internal backup battery prevents the terminal from being reset if you need to remove and replace the main battery pack. It retains RAM data and allows the real-time clock to remain operational for up to 30 minutes when the main battery pack is removed. If the terminal is left without the main battery pack for more than 30 minutes, the internal backup battery needs to be recharged to function according to its specifications.

Note: Data and programs stored in Flash memory are not lost even if the internal backup battery fails. However, you must reset the real-time clock; see Setting the Time and Date on page 2-9.

Charging

The internal backup battery is powered by the main battery pack. Therefore, charging the internal backup battery requires that the main battery pack be installed in the terminal and the terminal be connected to a charging device.

The internal backup battery must be fully charged before using the terminal for the first time. The initial charge cycle takes approximately eight hours. After that, if the internal backup battery becomes fully discharged of power, it requires a minimum of 10 hours of charging time to function normally.

Guidelines

Follow these guidelines to maximize the life of the Dolphin's internal backup battery:

- Keep a charged Li-Ion battery pack in the Dolphin terminal. The internal battery prematurely discharges if there is not at least a partially charged battery in the terminal.
- Keep the Dolphin terminal connected to power when the terminal is not in use.

Managing Battery Power

Data and files saved on the Dolphin 7900 terminal may be stored in RAM; therefore, maintain a continuous power supply to the terminal to help prevent data loss. Letting the backup battery become fully discharged causes the terminal to lose all data in RAM. The internal battery discharges prematurely if there is not at least a partially charged battery in the terminal. When you remove a battery pack, insert another charged battery pack in the Dolphin.

If the main battery is low and the terminal is in suspend mode, pressing the SCAN or Power button will not wake the Dolphin 7900 terminal; you must replace the discharged battery with a fully charged battery.

Default Low and Critical Battery Points

The navigation bar at the top of the screen displays battery warning icons when the main battery reaches a low and critical battery points. For details about these warning icons, see Status Icons on page 4-15. If the navigation bar does not contain a warning icon, then the battery is adequately charged.

The Dolphin 7900 ships with default low and critical battery points already programmed in the registry. The registry contains two DWORD settings in the **[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Power]** entry:

“LowBatt”=19 (25%)

This sets the Low battery point to 25 percent (19 hex = 25 decimal). The low battery setting is the point at which the user is notified that the battery is low. The user is notified only once for a low battery.

“CriticalBatt”=a (10%)

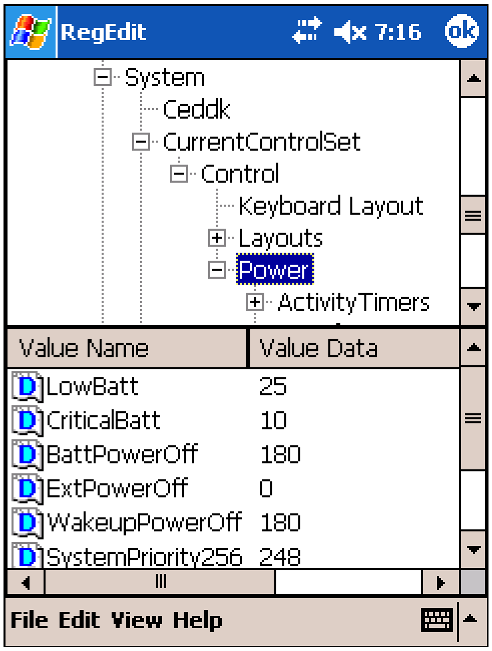
This sets the Critical Battery point to 10 percent (a hex = 10 decimal). The critical battery setting is the point at which the customer is warned that the battery charge is very low. This warning is posted every 3 minutes until the situation is corrected.

Note: Warnings do not appear when the terminal is on external power.

Setting Critical and Low Battery Points

Developers can re-reset the default battery points in the RegEdit utility under HHP Utils.

Tap **Start** > **HHP Utils** > **RegEdit**. In the RegEdit utility, drill-down to **HKEY_LOCAL_MACHINE** > **System** > **CurrentControlSet** > **Control** > **Power**. The Battery Points appear in the list.

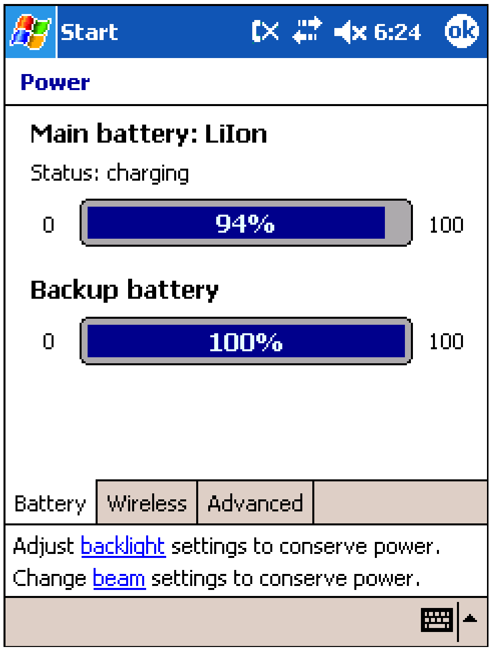


Value Name	Value Data
LowBatt	25
CriticalBatt	10
BattPowerOff	180
ExtPowerOff	0
WakeupPowerOff	180
SystemPriority256	248

Tap the Value Name to change the Value Data. You can reset the Value Data from 0 (no warning) to 99 (would nearly always warn). Tap **OK** to save changes.

Checking Battery Power

Tap **Start** > **Settings** > **System** tab **> Power**. The Battery tab opens displaying the charge status of both the installed Li-ion battery pack and the NiMH backup battery inside the terminal.



Power

Main battery: LiIon

Status: charging

0 94% 100

Backup battery

0 100% 100

Adjust backlight settings to conserve power.

Change beam settings to conserve power.

Power system settings contains three tabs: Battery, Wireless, and Advanced. For more information, see Power on page 7-11.

Storing Batteries

To maintain optimal battery performance, follow these storage guidelines:

- Avoid storing batteries outside the specified range of -4 to 104° F (-20 to 40°C) or in extremely high humidity.
- For prolonged storage, do not keep batteries stored in a charger that is connected to a power source.

Guidelines for Battery Use and Disposal

The following are general guidelines for the safe use and disposal of batteries:

- Use only the battery supplied, recommended, or approved by HHP.
- Replace defective batteries immediately; using a defective battery could damage the Dolphin terminal.
- Never throw a used battery in the trash. It contains heavy metals and should be recycled according to local guidelines.
- Don’t short-circuit a battery or throw it into a fire. It can explode and cause severe personal injury.
- Excessive discharge damages a battery. Recharge the battery when your terminal indicates low battery power.
- Although your battery can be recharged many times, it will eventually be depleted. Replace it after the battery is unable to hold an adequate charge.
- If you are not sure the battery or charger is working properly, please send it to HHP or an authorized HHP service center for inspection.

Dolphin 7900 Technical Specifications

System Architecture	
Processor:	Intel X-Scale PXA255 400MHz
Development Environment:	HHP Dolphin SDK Add-on for Pocket PC 2003 - supports Embedded Visual C++ 4.0 HHP Dolphin .NET SDK for Pocket PC 2002 and 2003 - supports Visual Studio.NET 2003 (VB.NET and C#.NET) HHP Dolphin GSM/GPRS SDK Add-on for Pocket PC 2003 - supports Embedded Visual C++ 4.0 and Visual Studio.NET 2003
Operating Platform:	Windows Mobile 2003 Second Edition Software for Pocket PCs - Professional Edition
Third-Party Software:	Support for Connect Terminal Emulation software (TNVT, 3270, 5250) and Java Virtual Machine (JVM) runtime, ITScriptNet Batch and Omni, MCL, and App Forge
Memory:	64MB RAM x 64MB non-volatile synchronous Flash standard; 128MB RAM high memory optional
Data Inputs	
Imager/Scanner:	See Image Engine Options on page 5-1.
1D Symbologies:	See 1D Symbologies on page 5-1.
2D Symbologies:	See 2D Symbologies on page 5-1.
Composite Codes	See Composite Codes on page 5-1.
OCR Fonts:	See OCR Codes on page 5-1.
Three Keyboard Options:	Two backlit keyboard options: 25-key numeric-shifted alpha, 36-key alpha-shifted numeric See Using Dolphin 7900 Keyboards on page 6-1.
Data Outputs	
Display:	See Display on page 3-3.
I/O Ports:	Industrial-grade mechanical connector supports communications-USB at 12Mbps, serial RS-232 up to 115Kbps- and charging via cradles or AC adapter cables, IrDA port-Integrated, Speaker-Integrated, Microphone-Integrated, Headset jack
Mass Storage:	User-accessible Mini Secure Digital (Mini-SD) memory interface
Wireless Radio Options	
WLAN:	IEEE 802.11b DSSS Authentication Methodologies: LEAP, MD5, TLS, TTLS, PEAP, and WEP
WWAN	GSM/GPRS Tri-band (900, 1800, 1900 MHz) or (850, 1800, 1900 MHz) radio with accessible SIM card interface
WPAN:	Bluetooth radio
Physical	
Dimensions:	7.3"L x 3. 5"W x 1.7"D max (185 x 89 x 43 mm), 3.2"W x 1.5"D at grip (81 x 38 mm)
Weight:	WLAN: 17.3 oz. (490 gm), WPAN: 17.1 oz. (484 gm), WLAN/WPAN: 17.4 oz. (493 gm)
Operating Temperature:	14 to 122°F (-10°C to 55°C) The terminal can operate in temperatures lower than -20°C with potential degradation in performance depending on the application
Storage Temperature:	-22 to 176°F (-30°C to 80°C)
Humidity:	95% humidity, non-condensing

Dolphin 7900 Technical Specifications

Electrical Static Discharge:	15 kv on all surfaces
Impact Resistance:	Withstands multiple 5ft. (1.5m) drops onto concrete
Environmental Resistance:	Independently certified to meet IP64 standards for moisture and particle resistance
Power:	Lithium-Ion battery technology – 7.4V, 14.8 watt-hour main battery with hot-swappable design for fast replacement in the field
Other:	Integrated stylus with optional tether and adjustable, removable hand strap
Peripherals/Accessories	
Dolphin HomeBase	Charging/communications cradle with auxiliary battery well. Data transfer via RS-232 serial or USB ports.
Dolphin Mobile Base	Mobile charging/communication cradle. Data transfer via RS-232 serial. Power out 5 volts for peripheral devices.
Dolphin QuadCharger	Four-slot battery charger that charges four batteries in under four hours. One slot doubles as a battery analyzer.
Dolphin Mobile Charger	Charges a Dolphin terminal by plugging into a vehicle cigarette lighter/power port.
Dolphin Net Base	Four-slot charging/communication cradle designed for Ethernet-based communications.
Dolphin ChargeBase	Four-slot charging cradle that holds, powers, and charges a terminal in each slot.
Charging/Comm Cables	USB or serial cables that charge and communicate with the terminal directly–without a cradle.
Li-Ion Battery Pack	7.4V, 14.8 watt hour Li-ion rechargeable main battery for the Dolphin.
Regulatory Approvals	
FCC-CE-Radio Country:	US/Canada, R&TTE

4

Using the Dolphin 7900

Overview

This chapter provides the basic instructions you need to operate the Dolphin 7900.

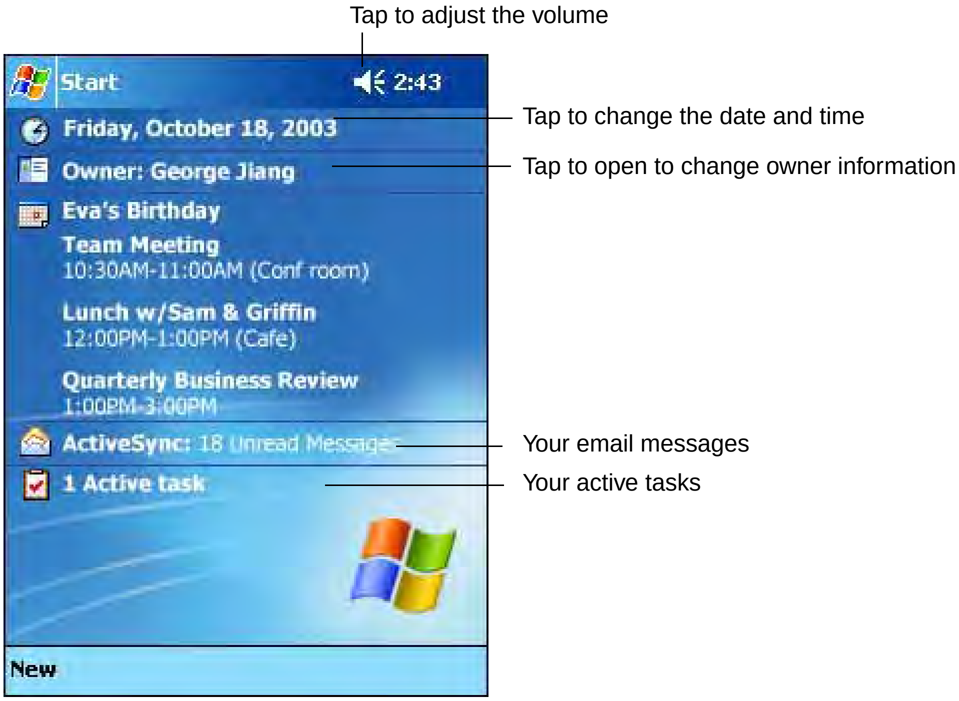
Using the Touch Screen

HHP recommends using screen protectors to protect the touch screen; especially when used with applications that require high-volume interfacing with the touch screen. Screen protectors help prevent damage to the touch screen display and are easily installed. Screen protectors can be purchased at any major computer retail store or directly from HHP.

⚠ *For touch screen input, use the included stylus or your finger. The method you choose depends on which one is appropriate for your application. While there is a great deal of variation in different applications, for buttons or icons that are close together, you generally achieve greater accuracy with the stylus. Use of other objects, such as paper clips, pencils, or ink pens can damage the input panel and will void the warranty.*

Today Screen

When the terminal powers one for the first time, you see the Today screen. You can also display it by tapping **Start** and then **Today**. On the Today screen, you can see at a glance important information for the day.



Start

2:43

Friday, October 18, 2003

Owner: George Jiang

Eva's Birthday

Team Meeting
10:30AM-11:00AM (Conf room)

Lunch w/Sam & Griffin
12:00PM-1:00PM (Cafe)

Quarterly Business Review
1:00PM-3:00PM

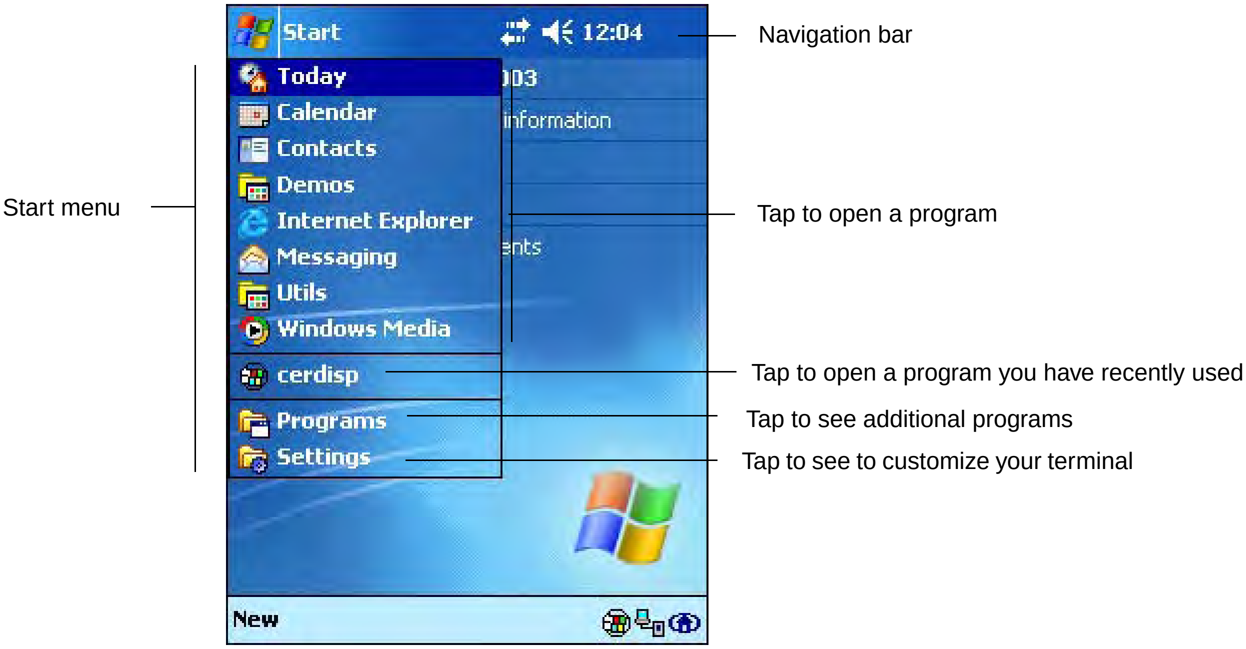
ActiveSync: 18 Unread Messages

1 Active task

New
Tap to adjust the volume
Tap to change the date and time
Tap to open to change owner information
Your email messages
Your active tasks

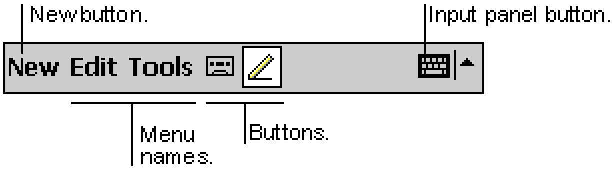
Navigation Bar

The navigation bar is located at the top of the screen and displays the active program and current time, and allows you to switch to programs and close screens.



Command Bar

Use the command bar at the bottom of the screen to perform tasks in programs. The command bar includes menu names, buttons, and the Input Panel button. To create a new item in the current program, tap **New**. To see the name of a button, tap and hold the stylus on the button. Drag the stylus off the button so that the command is not carried out.

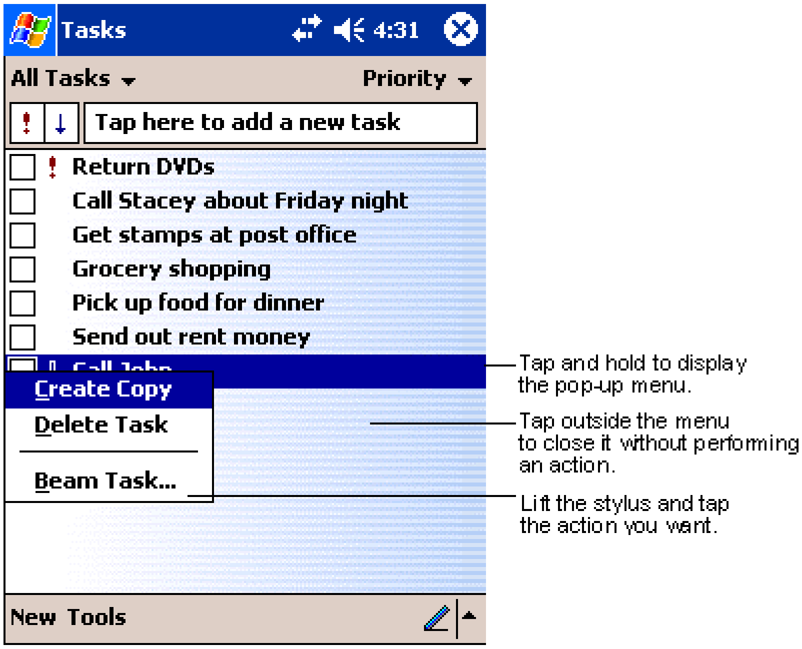


Pop-Up Menus

With pop-up menus, you can quickly choose an action for an item. For example, you can use the pop-up menu in the contact list to quickly delete a contact, make a copy of a contact, or send an e-mail message to a contact. The actions in the pop-up menus vary from program to program.

To access a pop-up menu,

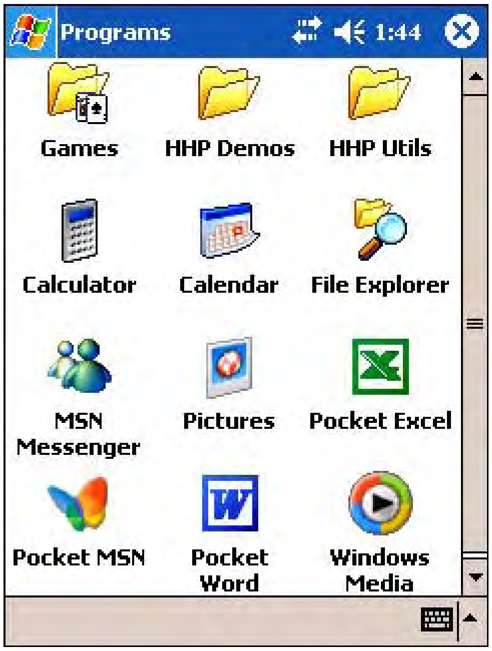
1. Tap and hold the stylus on the item name. The pop-up menu appears.
2. Lift the stylus, and tap the action you want to perform.


Tasks
4:31
All Tasks
Priority
Tap here to add a new task
Return DVDs
Call Stacey about Friday night
Get stamps at post office
Grocery shopping
Pick up food for dinner
Send out rent money
Call John
Create Copy
Delete Task
Beam Task...
New Tools
Tap and hold to display the pop-up menu.
Tap outside the menu to close it without performing an action.
Lift the stylus and tap the action you want.

Note: To close the menu without performing an action, tap the screen anywhere outside the menu.

Selecting Programs

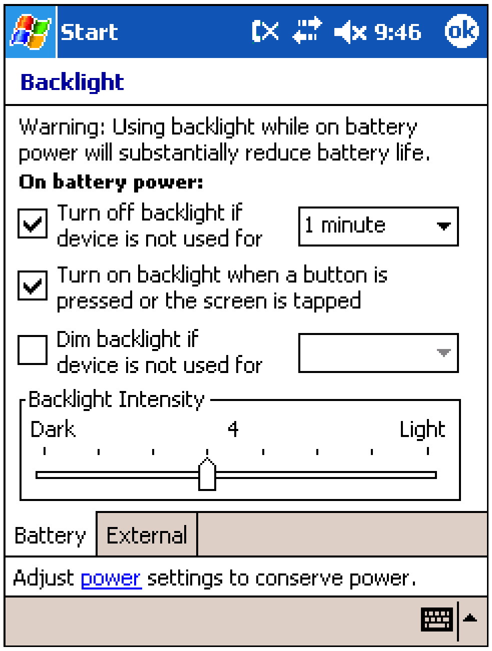
To see additional programs loaded on your terminal, tap **Start > Programs**. The Programs screen displays the programs that are not listed on the Start menu. To open a program, tap once on the icon.



Note: Some programs have abbreviated labels underneath the icon. To see the full spelling of an abbreviated label, tap and hold the stylus on the label. Drag the stylus off the label so that the command is not carried out.

Adjusting the Backlight

The backlight for the color display is user-defined. There are two tabs - one for Battery and the other for External power. The options on each tab are the same. Go to **Start** > **Settings** > **System** tab > **Backlight**. Backlight settings open displaying the Battery tab.



Backlight

Warning: Using backlight while on battery power will substantially reduce battery life.

On battery power:

☑ Turn off backlight if device is not used for: 1 minute

☑ Turn on backlight when a button is pressed or the screen is tapped

□ Dim backlight if device is not used for

Backlight Intensity: Dark 4 Light

Adjust power settings to conserve power.

The graphic on the right displays the default backlight settings for color display terminals on battery power.

From the **Turn off backlight…** drop-down list, select how many minutes you want to elapse before the backlight automatically turns off.

Select the **Turn on backlight…** option if you want the display backlight to turn on when the a button is pressed or the touch screen is tapped.

From the **Dim backlight if…** drop-down list, select how many minutes you want to elapse before the backlight dims.

Move the **Backlight Intensity** slider to set the intensity of the backlight.

Tap **OK** to save settings.

The display backlight functions according to the settings saved here.

Note: The External tab contains the same options for external power.

Communication Media Options

Mechanical Connector

The 17-pin, industrial-grade, mechanical connector on the bottom panel is designed to work only with HHP sold/manufactured communication and charging peripherals. Via these peripherals, the connector supports USB and RS-232 communications, enabling the user to connect the Dolphin 7900 terminal to external devices such as scanners and printers.

For more information about the connector, see Mechanical Connector on page 3-7.

IrDA Port

The IrDA port enables the Dolphin 7900 to transmit data via pulses of light to and from other IrDA-compliant devices, such as printers and PCs or to other Dolphin 7900 terminals.

For more information, see Using Infrared on page 8-6.

802.11b Radio

The Dolphin 7900 may be equipped with a WiFi®-compliant, interoperable 2.4 GHz 802.11b direct sequence spread spectrum wireless local area network (WLAN) radio.

For more information, see Wireless LAN Communications with 802.11b on page 9-1.

Bluetooth Radio

The Dolphin 7900 may be equipped with a Bluetooth wireless personal area network (WPAN) radio.

For more information, see Wireless PAN Communications with Bluetooth on page 10-1.

GSM/GPRS Radio

The Dolphin 7900 may be equipped with a GSM/GPRS wireless wide area network (WWAN) radio.

For more information, see Wireless WAN Communications with GSM/GPRS on page 11-1.

Software Communication Programs

Microsoft ActiveSync v3.7 or Higher

Microsoft ActiveSync is a tool that enables mobile computing devices, such as the Dolphin 7900, to exchange and synchronize application data with a desktop computer.

For more information, see Using ActiveSync on page 8-2.

RAS

Short for Remote Access Services, RAS is a feature built into Windows NT that enables users to log into an NT-based LAN using a modem, X.25 connection or WAN link. RAS is fully supported and allows the use of PPP or SLIP connections for network connectivity.

Radio Options

Dolphin 7900 terminals can be configured with one or a combination of the following radios:

- 802.11b
- Bluetooth
- GSM/GPRS

Available Radio Combinations

Dolphin 7900 terminals can be configured with more than one radio.

Co-located Radios

Some radio combinations are co-located, which means that you can use only one radio at a time. In this case, you can have both radios installed but need to power one up and the other down before operation.

- 802.11b and GSM/GPRS

Co-operational Radios

Some combinations are co-operational, which means that you can power up and operate both radios simultaneously.

- Bluetooth and 802.11b
- Bluetooth and GSM/GPRS

Radio Driver Installation

Radio drivers install during the autoinstall whenever the mobile computer is initialized; when first turned on or after a hard reset. Only the appropriate drivers for your terminal's radio configuration install. For example, if your terminal is configured only with an 802.11b radio, only the driver for that radio installs. For more information, see Autoinstall on page 2-9.

When a single radio installs, its radio driver is powered up automatically after initialization is complete. In general, when more than one radio installs, the terminal powers up the 802.11b radio. However, if a GSM radio is installed, the terminal powers up the GSM radio.

The Radio Manager

The Radio Manager is a control panel applet through which the radio power driver controls the radio state. It enables you to choose which radios on the terminal are powered up. When powered up, the radio is transmitting, when powered down, the radio is not transmitting.

Single Radio Configuration

If your terminal contains a single radio module and its associated driver is installed, operates by itself without any special configuration made to the device.

Multiple Radio Configuration

Configuration of simultaneous radio operation is done during the manufacturing process according to FCC regulations. If multiple radio modules are installed in your terminal, simultaneous operation must be configured on the device before the radio power driver allows it. In other words, verify which radio or radios are powered up or down.

Multiple Radio Operation

GSM and 802.11b are mutually exclusive. While they may both be present, they cannot be allowed to operate simultaneously. If you have modules and drivers for both radios installed on your terminal, you must ensure that one radio is powered down before using the other.

The Bluetooth radio is allowed to operate by itself or simultaneously with either of the GSM or 802.11b radios.

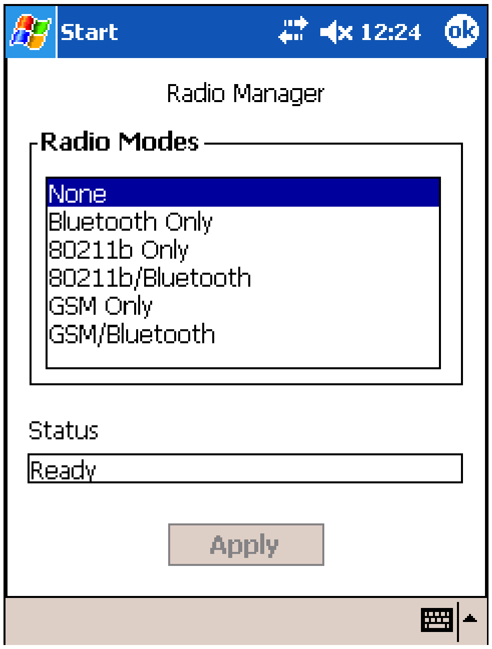
Powering Up Radios

Requirements

To successfully power up a radio, both the hardware module and the software driver must be installed on the terminal. If the module is present, the radio appears in the Radio Manager. However if the driver is not installed, you cannot successfully power up the radio. Attempting to do so produces an error in the Status field that tells you that the driver is not installed.

To Power Up a Radio or Radio Combination

1. Open the Radio Manager by going to **Start** > **Settings** > **Connections** tab > **Radio Manager**. The Radio Manager appears identifying which radio modules are installed. The highlighted entry is the radio mode that is currently enabled; its Status should be Ready.



2. Select the radio in the Radio Modes list and tap **Apply**.

The radio drivers are powered down and powered up in the proper sequence. For example, if the radio powered up is Bluetooth Only and you try to switch to 802.11b Only, after **Apply** is tapped, the Radio Manager powers down the Bluetooth radio first, then powers up the 802.11b radio.

If an error occurs during this process, the radio mode change is abandoned. The resulting radio state is the status of the radios at the time the error occurred.

Radio Modes The Radio Modes section displays the radio hardware modules currently installed on the terminal. For example, if a working Bluetooth module is installed, the box contains the line Bluetooth Only whether or not that radio is currently powered up.

Status field The Status field provides feedback on the state of the radio. When it reads “Ready,” the radio selected in the Radio Modes box is powered up. The Status field displays error messages when a radio cannot be enabled.

Powering Down Radios

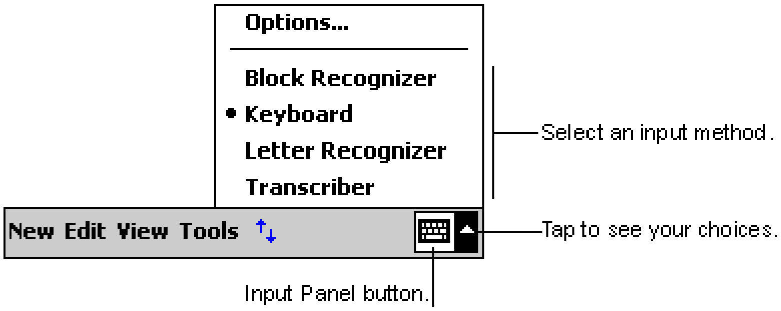
Radio drivers are automatically powered down if the radio or radio combination that is currently powered up requires it. To power down all radios, select None and tap **Apply**.

For more information about 802.11b radios, see Wireless LAN Communications with 802.11b on page 9-1.
For more information about Bluetooth radios, see Wireless PAN Communications with Bluetooth on page 10-1.
For more information about GSM/GPRS radios, see Wireless WAN Communications with GSM/GPRS on page 11-1.

Using the Soft Input Panel (SIP)

Use the SIP to enter information in any program on the Dolphin terminal. You can either type on the soft keyboard or write on the touch screen using Letter Recognizer or Block Recognizer. In either case, the characters appear as typed text on the screen.

To show or hide the SIP, tap the **Input Panel** button. Tap the arrow next to the Input Panel button to see your choices.

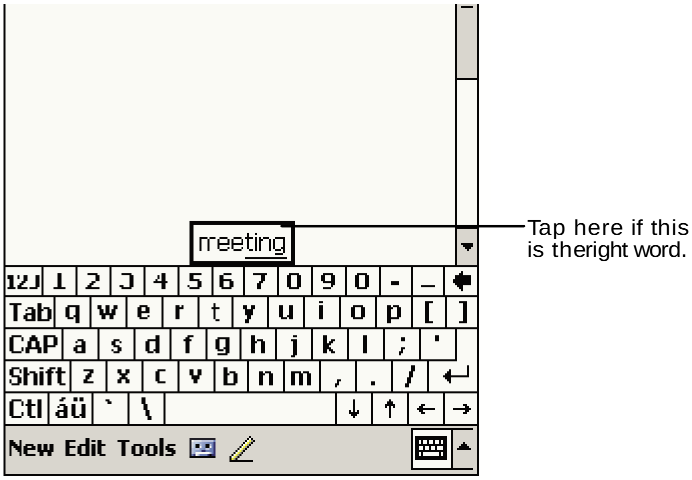


When you use the SIP, your terminal anticipates the word you are typing or writing and displays it above the input panel. When you tap the displayed word, it is inserted into your text at the insertion point. The more you use your Dolphin 7900 terminal, the more words it learns to anticipate.

To change word suggestion options, such as the number of words suggested at one time, tap **Start** > **Settings** > **Personal** tab > **Input** > **Word Completion** tab.

Using the SIP Keyboard

1. Tap the arrow next to the Input Panel button and select **Keyboard**.
2. On the soft keyboard that is displayed, tap the keys with your stylus.

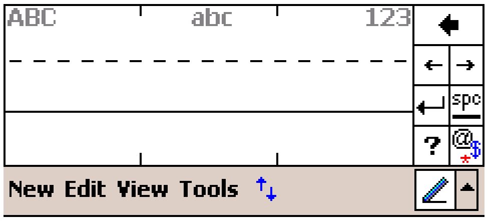

meeting
Tap here if this is theright word.
123 1 2 3 4 5 6 7 8 9 0 - =
Tab q w e r t y u i o p [ ]
CAP a s d f g h j k l ; '
Shift z x c v b n m , . /
Ctl áü ` \ ↓ ↑ ← →
New Edit Tools

Using the Letter Recognizer

With Letter Recognizer you can write letters using the stylus just as you would on paper.

1. Tap the arrow next to the Input Panel button and then **Letter Recognizer**.

2. Write a letter in the box.

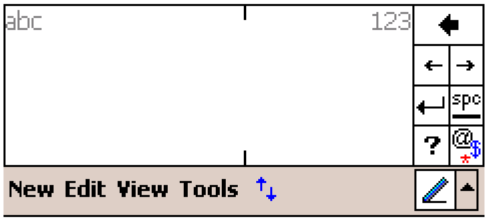


When you write a letter, it is converted to typed text that appears on the screen. For specific instructions on using Letter Recognizer, with Letter Recognizer open, tap the question mark next to the writing area ?.

Using the Block Recognizer

With Block Recognizer you can input character strokes using the stylus.

1. Tap the arrow next to the Input Panel button and then **Block Recognizer**.
2. Write a letter in the box.



When you write a letter, it is converted to typed text that appears on the screen. For specific instructions on using Block Recognizer, with Block Recognizer open, tap the question mark next to the writing area.

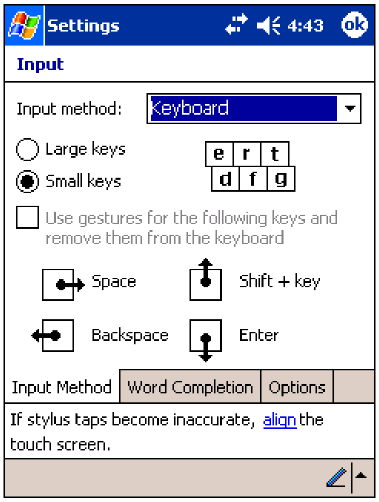
Selecting Text

To edit or format typed text, select it by dragging the stylus across the text. Then, use the commands on the pop-up menu to cut, copy, and paste the selected text.

Input Panel Options

You can set input options by going to **Start** > **Settings** > **Personal** tab > **Input**.The following graphics are the tab windows where you can customize the input panel to your preferences:

Input Method tab



Input method: Keyboard

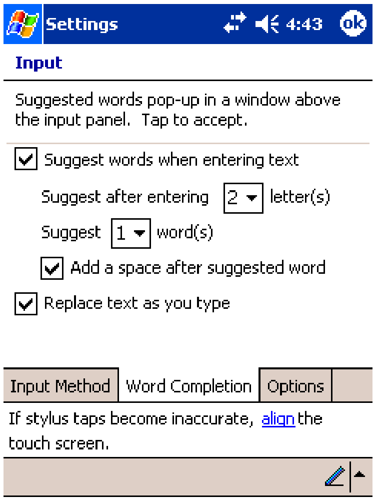
○ Large keys

● Small keys

□ Use gestures for the following keys and remove them from the keyboard

If stylus taps become inaccurate, align the touch screen.

Word Completion tab



Suggested words pop-up in a window above the input panel. Tap to accept.

☑ Suggest words when entering text

Suggest after entering 2 letter(s)

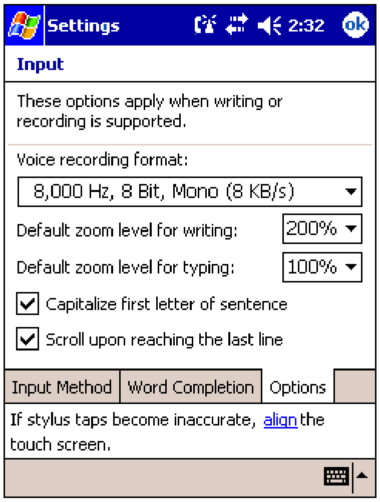
Suggest 1 word(s)

☑ Add a space after suggested word

☑ Replace text as you type

If stylus taps become inaccurate, align the touch screen.

Options tab



These options apply when writing or recording is supported.

Voice recording format: 8,000 Hz, 8 Bit, Mono (8 KB/s)

Default zoom level for writing: 200%

Default zoom level for typing: 100%

☑ Capitalize first letter of sentence

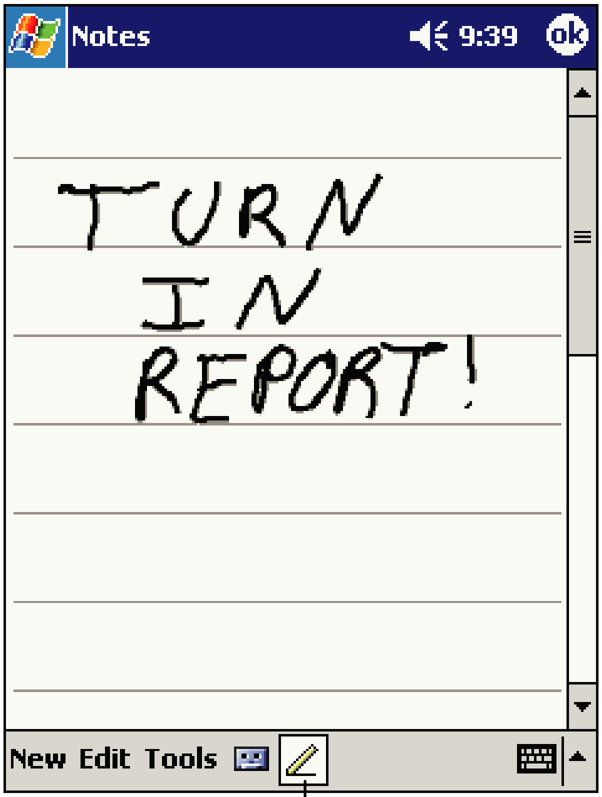
☑ Scroll upon reaching the last line

If stylus taps become inaccurate, align the touch screen.

Writing on the Screen

In any program that accepts writing, such as the Notes program, and in the **Notes** tab in Calendar, Contacts, and Tasks, you can use your stylus to write directly on the screen as you would on paper.

To write on the screen, tap the **Pen** button to switch to writing mode. This action displays lines on the screen to help you write.



Tap the Pen button and use your stylus like a pen .

Note: Some programs that accept writing may not have the Pen button. See the documentation for that program to find out how to switch to writing mode.

To Select Writing

If you want to edit or format writing, you must select it first.

1. Tap and hold the stylus next to the text you want to select until the insertion point appears.
2. Without lifting, drag the stylus across the text you want to select.

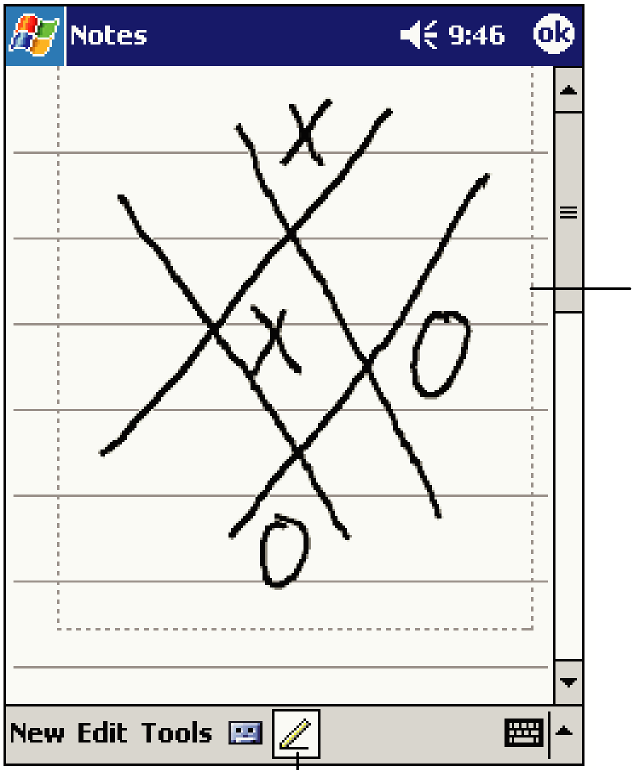
If you accidentally write on the screen, tap **Tools,** then **Undo** and try again. You can also select text by tapping the **Pen** button to deselect it and then dragging the stylus across the screen.

You can cut, copy, and paste written text in the same way you work with typed text: tap and hold the selected words and then tap an editing command on the pop-up menu, or tap the command on the **Edit** menu.

Drawing on the Screen

Drawing on the screen is similar to writing on the screen. The difference between writing and drawing on the screen is how you select items and how they can be edited. To create a drawing, cross three ruled lines on your first stroke. A drawing box appears. Subsequent strokes in or touching the drawing box become part of the drawing. Drawings that do not cross three ruled lines will be treated as writing.

For example, selected drawings can be resized, while writing cannot.



The drawing box indicates the boundaries of the drawing.

Pen button.

Note: You may want to change the zoom level so that you can more easily work on or view your drawing. Tap **Tools** and then a zoom level.

Selecting a Drawing

To edit or format a drawing, tap and hold the stylus on the drawing until the selection handle appears. To select multiple drawings, deselect the Pen button and then drag to select the drawings you want.

You can cut, copy, and paste selected drawings by tapping and holding the selected drawing and then tapping an editing command on the pop-up menu, or by tapping the command on the Edit menu. To resize a drawing, make sure the Pen button is not selected, and drag a selection handle.

Status Icons

Status Icon	Meaning
🔈	Turns all sounds on and off
🔋	Backup battery is low
🔌	Main batteries are charging
🪫	Main batteries are low
!	Main batteries are very low
🔋	Main batteries are full
⟳	Synchronization is beginning or ending
✉	Notification that one or more e-mail messages were received

Note: The Notification icon 💬 displays if more notification icons need to be displayed than there is room to display them. Tap the icon to view all notification icons.

Notifications

Notifications remind you when you have something to do. For example, if you've set up an appointment in Calendar, a task with a due date in Tasks, or an alarm in Clock, you'll be notified in any of the following ways:

- A message box appears on the screen.
- A sound, which you can specify, is played.

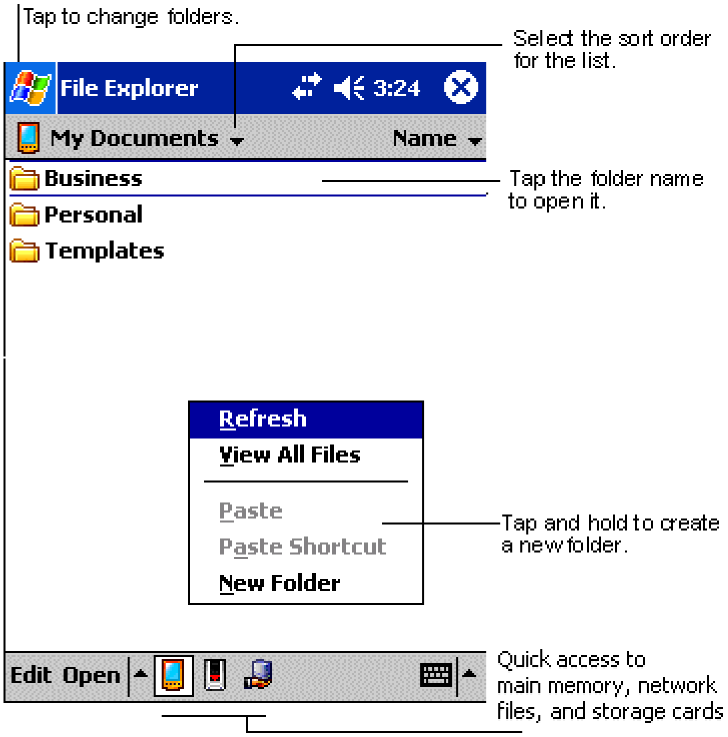
To choose reminder types and sounds, tap **Start** > **Settings** > **Personal** tab > **Sounds & Notifications** (see Personal Tab on page 7-2). The options you choose here apply throughout the terminal.

Finding and Organizing Information

The Find feature on your Dolphin mobile computer helps you quickly locate information. On the **Start** menu, tap **Find**. Enter the text you want to find, select a data type, and then tap **Go** to start the search.

To quickly find information that is taking up storage space, select **Larger than 64 KB** in **Type**.

You can also use the File Explorer to find files and organize these files into folders. On the **Start** menu, tap **Programs**, and then **File Explorer**.


Tap to change folders.
Select the sort order for the list.
File Explorer
3:24
My Documents
Name
Business
Personal
Templates
Tap the folder name to open it.
Refresh
View All Files
Paste
Paste Shortcut
New Folder
Tap and hold to create a new folder.
Edit Open
Quick access to main memory, network files, and storage cards

You can move files in File Explorer by tapping and holding the item you want to move, and then tapping **Cut** or **Copy** and **Paste** on the pop-up menu.

5

Using the Image Engine

Overview

The Dolphin 7900 terminal houses a compact image engine that instantly reads all popular 1D and 2D bar codes and supports omni-directional aiming and decoding for greater flexibility in real-world settings. The image engine can also capture digital images, such as signatures and pictures of damaged inventory. Images are saved in industry-standard file formats.

Image Engine Options

Dolphin 7900 terminals may be equipped with one of the following image engines:

- IMAGETEAM™ 4100SR with green aimer, decodes from 2.5 to 12.5 in. (6.3 to 32 cm.)
- IMAGETEAM™ 4100SF with green aimer, decodes from 2.1 to 8.9 in. (5 to 22.6 cm.)
- IMAGETEAM™ 4100HD with green aimer, decodes from 2.2 to 6.5 in. (5.6 to 16.5 cm)

Note: Specifications are for 100% UPC Code.

Bar Code Symbologies Supported

The Dolphin 7900 supports the following bar code symbologies:

Symbology type	Symbologies supported
1D Symbologies	Codabar Code 3 of 9 Code 11 Code 32 Pharmaceutical (PARAF) Code 93 Code 128 EAN with Add-On and EAN with Extended Coupon Code EAN-13 Interleaved 2 or 5 Matrix 2 of 5 Plessey PosiCode RSS Straight 2 of 5 IATA Straight 2 of 5 Industrial Telepen Trioptic Code UCC/EAN-128 UPC and UPC-A
2D Symbologies	Aztec Code 16K Composite Data Matrix MaxiCode OCR PDF417 QR Code RSS
Composite Codes	Aztec Mesa Codablock F EAN·UCC RSS-14
OCR Codes	OCR-A and OCR-B

Postal Codes	Postnet and most international 4 state codes Australian Post British Post Canadian Post China Post Japanese Post KIX (Netherlands) Post Korea Post Planet Code

Activating the Engine

The Dolphin 7900 offers the following options to activate the engine:

- The Scan key located in the center of both keyboards for easy access from either hand - see SCAN key on page 6-5.
- The Scan buttons located on both side panels for easy one-hand scanning - see Scan Button on page 3-6.

Demos

All Dolphin 7900 terminals contain Demos that enable you to test and verify the image engine. To access these demos, go to **Start** > **Demos**,

- Select **Image Demo** to verify imaging, or
- Select **Scan Demo** to verify decoding.

Decoding

The Dolphin 7900 terminal supports two types of image decoding for use in various bar code reading and imaging applications: full-area imaging and Advanced Linear Decoding (ALD).

Full-area Imaging

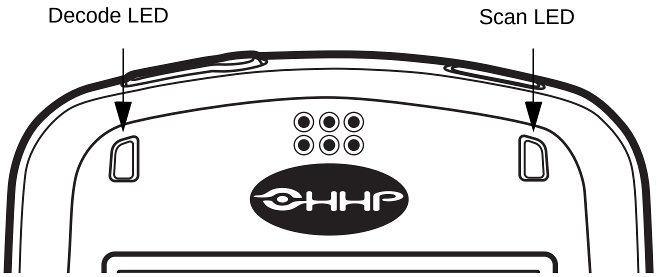
Full-area imaging provides omni-directional reading of linear and non-linear 1D and 2D bar codes, OCR, signature capture, and picture taking. When reading all bar code types using full-area imaging, a positive read can be obtained from many positions; see Scanning Position Options on page 5-3. To achieve the best read, the aiming beam should be centered horizontally across the bar code.

ALD

ALD provides fast reading of linear and stacked linear bar codes. To achieve a positive read when reading linear 1D and PDF417 bar codes, the green aiming beam should be centered horizontally across the bar code. When ALD is enabled, the reader does not read matrix or postal codes.

To Decode a Bar Code

1. Position the Dolphin 7900 terminal over the bar code. The imager has a slight downward angle. A range of 4-10 inches (10-25 cm) from the bar code is recommended.
2. Project the imager's aiming beam by pressing and holding the SCAN key or the Scan button.
3. The scan LED lights red.

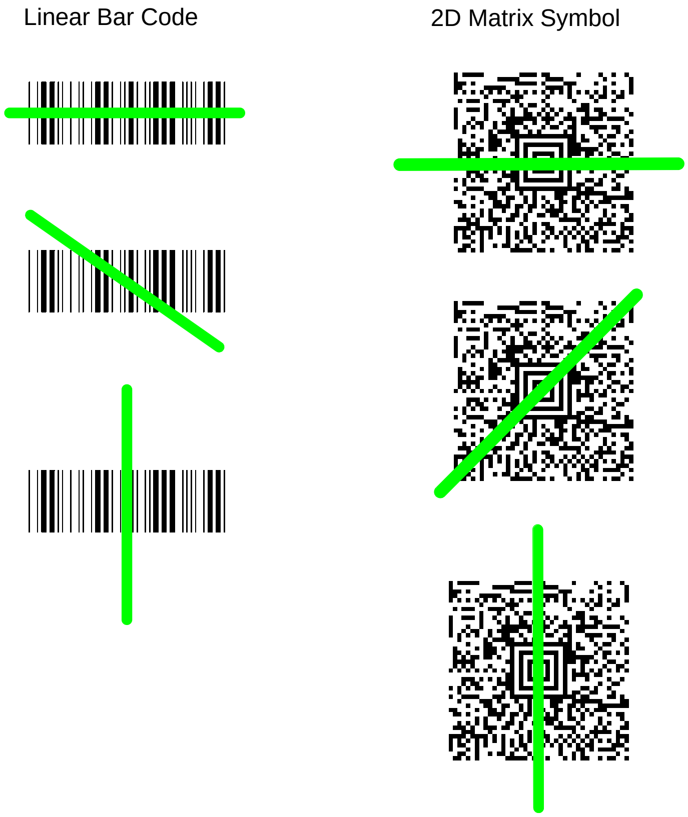


4. Center the aiming beam over the bar code. The aiming beam should be oriented in line with the bar code to achieve optimal decoding (see Scanning Position Options on page 5-3).
5. Release the Scan key or Scan button.
6. When the bar code is successfully decoded, the decode LED lights green and the terminal beeps.
7. The bar code information is entered into the application in use.

Scanning Position Options

The aiming beam is smaller when the terminal is held closer to the code and larger when it is farther from the code. Symbologies with smaller bars or elements (mil size) should be read closer to the unit. Symbologies with larger bars or elements (mil size) should be read farther from the unit.

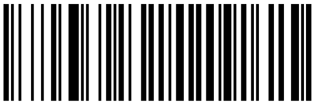
The following chart displays the imager’s aiming positions:



Sample Bar Codes

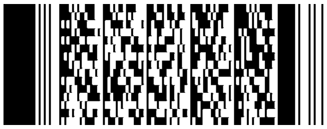
You can use the following bar codes to verify decoding:

Sample 128



Code 128

Sample PDF417



PDF417 Test Message

Capturing Images

The image-capture process is an intuitive, split-second operation for experienced users. By following the basic guidelines, new users can easily develop their own technique and, with practice, quickly learn to adapt it to different application environments.

Image Preview

When the imaging process is initiated, the Dolphin 7900 touch screen displays a preview of the object. This is a live video image of what the imager is currently viewing and has a slightly degraded appearance compared to the captured image. This is normal.

Image Files

The terminal is capable of saving images in a number of industry-standard file formats such as *.bmp, *.jpg and *.png. The default file format for images is a grayscale *.jpg. To obtain the highest quality images, take grayscale images.

Digital images have a maximum image size of 640 x 480 pixels and may have up to a 256 grayscale image definition. The image quality and related file size are determined by the data compression method used by the software application used to take images. The average size of the image file is approximately 4-8K. However, the size of the image depends on the content of the image - the more complex the content, the larger the file size.

Taking an Image

The following steps are basic guidelines for taking images:

1. Point the Dolphin 7900 terminal at the object. The imager has a slight downward angle.
2. To preview the image before capturing, press and hold the SCAN key or the Scan button.
3. The touch screen displays a preview of the object, and the decode and scan LEDs light red.
4. Adjust the terminal's position until the object appears on the screen the way you want it to appear in the image.
5. Hold the terminal still and release the SCAN key or Scan button.
   The scan and decode LEDs flash red, the touch screen flashes, and the captured image appears on the screen.

6. Unless otherwise specified by the application in use, the image is saved to the My Device folder (Start > Programs > File Explorer > My Device).

Uploading Images

Image files can be uploaded to a host PC via

- Microsoft ActiveSync and a Dolphin communication peripheral, or
- Over your wireless radio network.

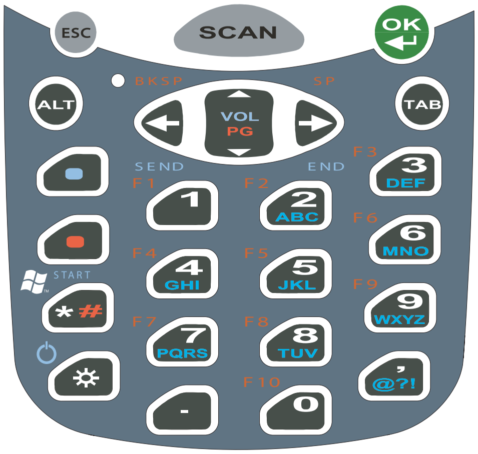
6

Using Dolphin 7900 Keyboards

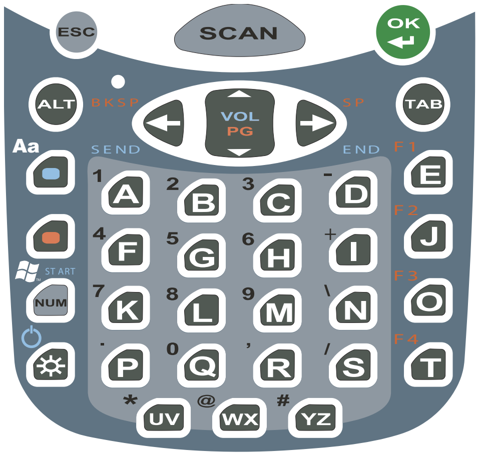
Overview

The Dolphin 7900 series features two keyboard options: 25-key numeric-alpha keyboard and 36-key alpha-numeric keyboard.

25-key Numeric-Alpha Keyboard



36-key Alpha-Numeric Keyboard



Both keyboards are recessed under the overlay for maximum durability and backlit for maximum viewability in various lighting conditions. Keyboard overlays are color-coded to indicate the functions performed or characters typed when the color-coded key is pressed immediately after the Red or Blue Modifier key.

In addition to the standard number and letter keys, both keyboards contains three types of keys:

1. Function Keys
2. Navigation Keys
3. Modifier Keys

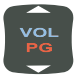
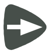
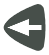
Using the Function Keys

Function keys are those keys that perform specific functions and usually have the name of the function they perform.

Name	Key	Function
SCAN	SCAN	The SCAN key activates the scan and wakes the terminals from suspend mode. Its position allows convenient one-handed image-taking and/or bar code decoding.
OK	OK ↵	The OK key confirms data entry and functions as an Enter key. Pressing the OK key also wakes the terminal from suspend mode.
Backspace (BKSP)	BKSP ←	The Backspace function is performed by pressing the Red modifier key + the left arrow. Backspace moves the cursor back one space and deletes each time the key combination is pressed. If you are typing text, a character is deleted each time you backspace.
Space (SP)	SP →	The Space function is performed by pressing the Red modifier key + right arrow. The Space key moves the cursor one space forward. If you are typing text, it moves the text one space forward as well.
Escape (ESC)	ESC	The Escape key performs a cancel action.
Backlight	☼	The Backlight key turns the keyboard backlight on and off.
Tab	TAB	The Tab key moves the cursor to the next tab stop or the next control (on a form).
Power	⏻ ☼	The Power function is performed by pressing the Blue modifier key + the Backlight key. Pressing this key combination powers on the terminal and puts a terminal already on in suspend mode.

Using the Navigation Keys

Located in the center of each keyboard for easy access with either hand, the navigation keys enable you to navigate the cursor through an application screen.

Press	To ...
	Move the cursor up one row or line. Move the cursor down one row or line.
	Move the cursor one character to the right.
	Move the cursor one character to the left.

The up and down arrows can be used for

- Volume up and down commands when pressed in combination with the blue modifier key, or
- Page up and page down commands when pressed in combination with the red modifier key.

Other functionality varies according to the application in use.

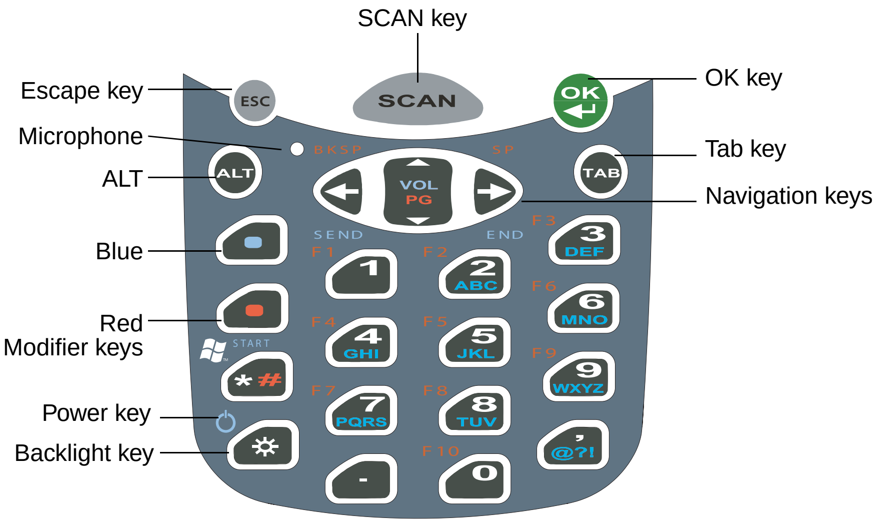
Using the Modifier Keys

Modifier keys are those keys that modify the next key pressed. They are used on combination with the keys that follow to perform functions or type special characters. In addition to the standard ALT key, the Dolphin 7900 terminal features Blue and Red modifier keys and a color-coded overlay.

Name	Key	Function
ALT	ALT	The function of the ALT key depends on the software application in use and the keys combination pressed.
Blue	🟦	The blue and red keys are used in combination with other keys to type special characters and perform system functions. Each key modifies only the next key pressed.
Red	🟥	The overlay of each keyboard is color-coded to indicate the character typed or function performed when specific keys are pressed immediately after the blue or red modifier key.

25-Key Numeric-Alpha Keyboard

The following graphic displays the 25-key numeric/alpha keyboard.



Alpha Mode Functionality

The 25-key keyboard defaults to numeric mode. Numeric mode is when you type numbers with the number keys. Alpha mode is when you type letters with number keys. On the number keys, there are alpha indicators that specify the letter(s) that will be typed when you press that key in combination with the Blue modifier key.

Please note that when typing in alpha mode, you must use the same multi-press method you would use when typing letters on a phone keypad. Each key press will type the next letter in the sequence as displayed in the alpha indicator.

Note: On the 25-key keyboard, alpha mode is achieved using Blue Modifier key combinations.

Blue Key Combinations

Characters

Key Combination	Character
Blue + 2	ABC
Blue + 3	DEF
Blue + 4	GHI
Blue + 5	JKL
Blue + 6	MNO
Blue + 7	PQRS
Blue + 8	TUV
Blue + 9	WXYZ
Blue + ,	@ ? !

Functions

Key Combination	Function
Blue + Backlight	Power
Blue + Left Arrow	Send
Blue + Right Arrow	End
Blue + Up Arrow	Volume up
Blue + Down Arrow	Volume down

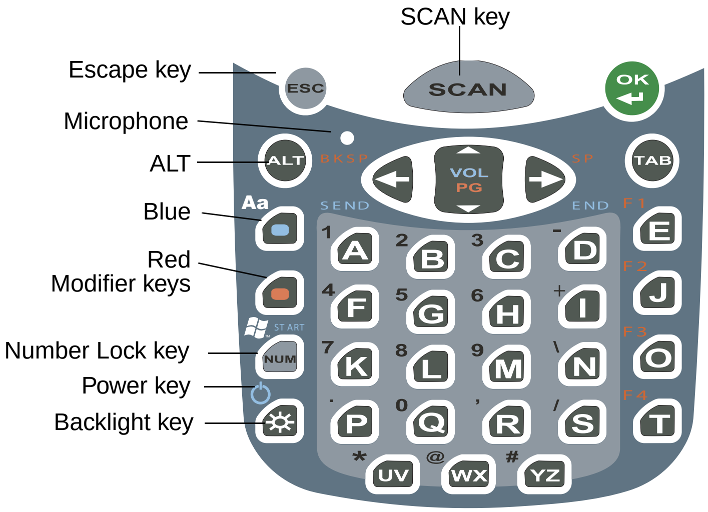
Red Key Combinations

Key Combination	Function/Special Character
Red + Left Arrow	Backspace
Red + Right Arrow	Space
Red + Up Arrow	Page up
Red + Down Arrow	Page Down
Red + ESC	Soft reset (warm boot)
Red + TAB	Hard reset (cold boot)
Red + 1	F1
Red + 2	F2
Red + 3	F3
Red + 4	F4
Red + 5	F5
Red + 6	F6
Red + 7	F7
Red + 8	F8

Key Combination	Function/Special Character
Red + 9	F9
Red + *	#

36-Key Alpha-Numeric Keyboard

The following graphic displays the 35-key alpha/numeric keyboard.



Number Mode Functionality

The 35-key keyboard defaults to alpha mode. Alpha mode is when you type letters with the letter keys. Numeric mode is when you type numbers with letter keys. On the alpha keys, there are numeric indicators that specify the number that will be typed when you press that key in combination with the Blue modifier key.

Please note that when typing in numeric mode, you must use the same multi-press method you would use when typing letters on a phone keypad. Each key press will type the next letter in the sequence as displayed in the alpha indicator.

Blue Key Combinations

Key Combination	Function/Special Character
Blue + Backlight	Power
Blue + Left Arrow	Send
Blue + Right Arrow	End
Blue + Up Arrow	Volume up
Blue + Down Arrow	Volume down

Red Key Combinations

Key Combination	Function/Special Character
Red + Left Arrow	Backspace
Red + Right Arrow	Space
Red + ESC	Soft reset (warm boot)
Red + TAB	Hard reset (cold boot)
Red + E	F1
Red + J	F2
Red + O	F3
Red + T	F4

NUM Key Combinations

Pressing the NUM lock key switches the keyboard to numeric mode where you can type numbers and special characters with the letter keys. You do NOT need to press and hold the NUM key when pressing the next key.

Key Combination	Function/Special Character
NUM + A	1
NUM + B	2
NUM + C	3
NUM + D	-
NUM + F	4
NUM + G	5
NUM + H	6
NUM + I	+
NUM + K	7
NUM + L	8
NUM + M	9
NUM + N	\
NUM + P	.
NUM + Q	0
NUM + R	,

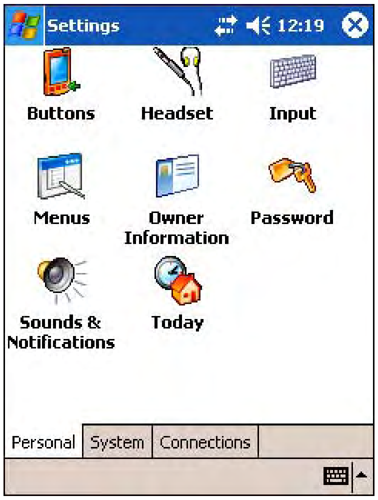
Key Combination	Function/Special Character
NUM + S	/
NUM + UV	*
NUM + WX	@
NUM + YZ	#

7 Settings

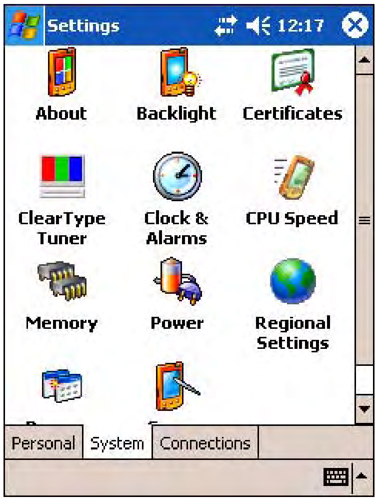
Overview

Customized settings are available on the Start menu. Go to **Start** > **Settings** and settings screen opens displaying the Personal tab. Settings consists of three tabs: Personal, System, and Connections.

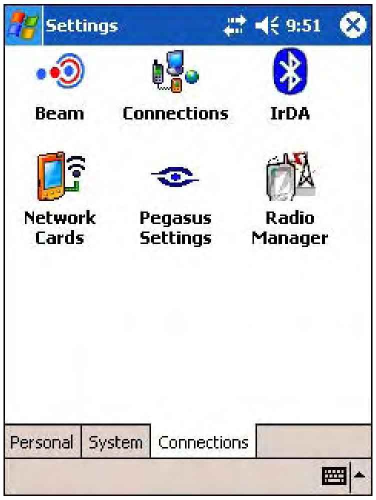
Personal Tab



System Tab



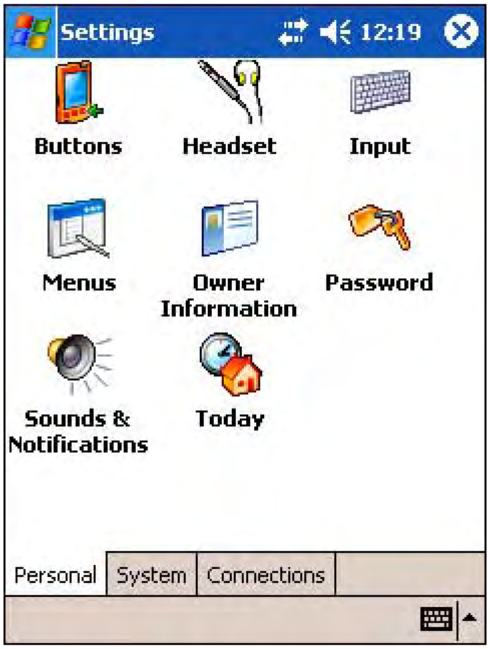
Connections Tab



Tab	This tab enables you to …
Personal	Customize buttons, set SIP options, and adjust headset settings; see Personal Tab on page 7-2.
System	Adjust system settings; see System Tab on page 7-6.
Connections	Establish network connections settings; see Connections Tab on page 7-20.

Personal Tab

To access the Personal tab, go to **Start** > **Settings**. The screen opens displaying the Personal tab.



Icon	**Tapping this icon enables you to …**
Buttons	Customize buttons to perform functions. To use this setting, the HotKeys HHP Utility must be initialized. Tap **Start** > **Utils** > **HotKeys** (the icon is the same). The HotKeys utility initializes. Return to the Personal tab and tap **Buttons**.
Headset	Adjust audio settings for headset use; see Headset Control on page 7-5.
Input	Customize the SIP. For details, see Input Panel Options on page 4-12.
Menus	Customize what appears on the Start and New menus; see Adding a Program to the Start Menu on page 7-3.
Owner Information	Enter your contact information. This information will appear on the Today screen.
Password	Password protect the terminal to limit access to your device.
Sounds & Notifications	Set the sound volume, enable and disable sounds for specific actions, and set sound parameters for system notifications.
Today	Customize the look and the information that is displayed on the Today screen

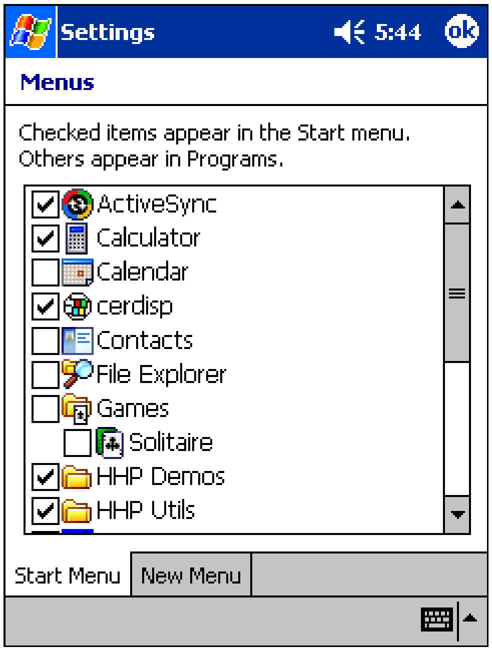
Note: Personal settings are stored in RAM memory. They are replaced by system defaults after each hard reset. For more information about resets, see Soft Reset (Warm Boot) on page 2-11.

Adding a Program to the Start Menu

You can add existing programs you use often, such as File Explorer, to the Start menu for faster access. You are not installing the program, just re-routing access to it.

Using System Settings

1. Tap **Start** > **Settings > Personal** tab **> Menus** > **Start Menu** tab.



Menus

Checked items appear in the Start menu.
Others appear in Programs.

- ☑ ActiveSync
- ☑ Calculator
- ☐ Calendar
- ☑ cerdisp
- ☐ Contacts
- ☐ File Explorer
- ☐ Games
  - ☐ Solitaire
- ☑ HHP Demos
- ☑ HHP Utils

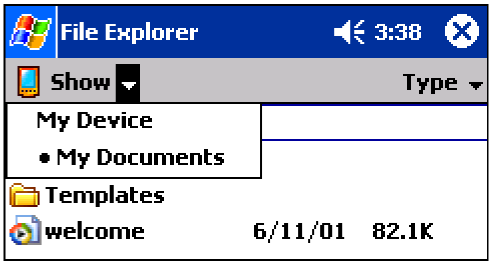
2. Tap the check box for the program you want to add and tap **OK** to save.
3. Tap the **Start** menu.
4. Verify that the program appears.

Using File Explorer

If you do not see the program listed, you can either use File Explorer to move the program or ActiveSync on the desktop computer to create a shortcut to the program and place the shortcut in the Start Menu folder.

Note: We recommend that you Copy and Paste Shortcut so that you do not alter your program configurations by accident. Using Copy and Paste Shortcut (as opposed to Cut and Paste) ensures that the program files remain where they need to be for the system to find them to perform system functions.

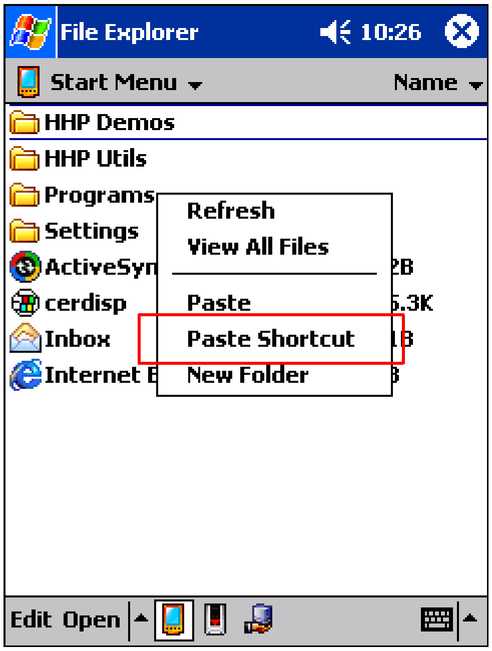
1. Tap **Start** > **Programs** > **File Explorer**, and navigate to the program.
   File Explorer opens to My Documents by default; to see a list of all folders, tap the folder name and then **My Device**.



Templates
welcome 6/11/01 82.1K

2. Tap and hold on the program, then tap **Copy** on the pop-up menu.

3. Navigate to the Windows folder and open the Start Menu (**My Device** > **Windows** > **Start Menu**), tap and hold a blank area of the window, and tap **Paste Shortcut** on the pop-up menu.



4. Tap the **Start** menu.

5. Verify that the program now appears.

Using ActiveSync on the Desktop Computer

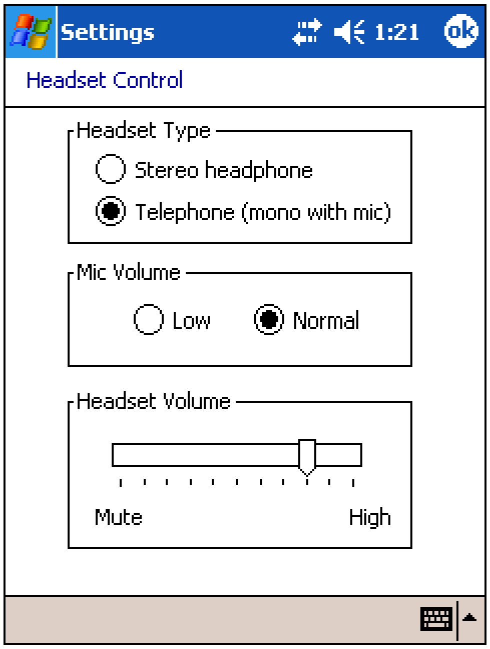
Here, you are performing the same basic process as on the terminal, except that you are using the Explore (Windows Explorer) utility to cut and paste.

1. Open **ActiveSync > Explore**.
2. Navigate to the program.
3. Right-click on the program and select **Create Shortcut**.
4. Select the shortcut, right-click, and select **Cut**.
5. Navigate to the **Start Menu** folder (Windows > Start Menu).
6. Right-click on an empty area and select **Paste**.
7. On the terminal, tap the **Start** menu.
8. Verify that program appears.

For more information, see ActiveSync Help.

Headset Control

The Headset Control setting enables you to adjust audio settings while using a headset.



Headset Control

Headset Type

○ Stereo headphone

● Telephone (mono with mic)

Mic Volume

○ Low ● Normal

Headset Volume

Mute High

Headset Type

Stereo headphone Select this option if you are using a headset for audio output only. In this case, you need to use the microphone on the terminal (Microphone, page 3-2) for audio input; i.e., listen via the headset and speak into the microphone. These types of headsets usually contain two earpieces for stereo sound. Tap **OK** to save your selection.

Telephone (mono with mic)

Select this option if you are using a headset that also contains a microphone. When this option is selected, you speak into the microphone on the headset and not the microphone on the terminal. These types of headsets usually have one earpiece for mono audio.
Tap **OK** to save your selection.

Mic Volume

These options enable you to adjust the audio level of the microphone. Normal is the default setting. If this is too loud for the listener, you can change the setting to Low.

These settings apply to the selected Headset Type. When you select Stereo headphone, the volume on the terminal's microphone (Microphone, page 3-2) adjusts. When you select Telephone (mono with mic), the volume on the headset's microphone adjusts.

This Mic Volume setting does not work if you are using a GSM radio for two-way voice communication. For more information about microphone volume with GSM, see Settings Menu on page 11-11.

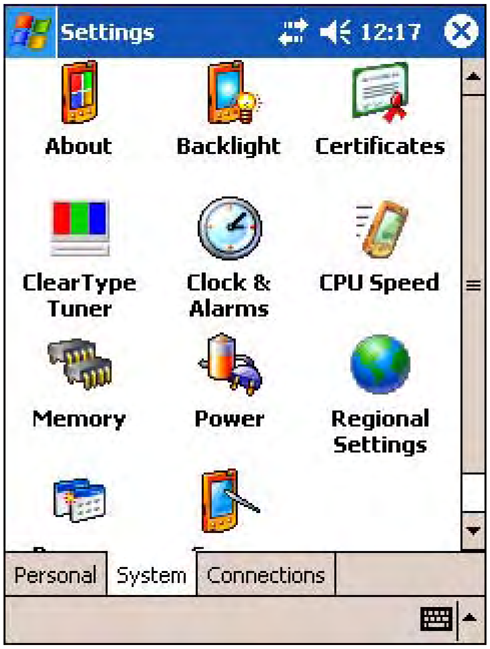
Tap **OK** to save your selection.

Headset Volume

This slider enables you to adjust the speaker volume (audio output) of the headset. Move the slider from Mute to High depending on your preference. The volume adjusts automatically as you move the slider. These headset volume settings apply to both Headset Types.

System Tab

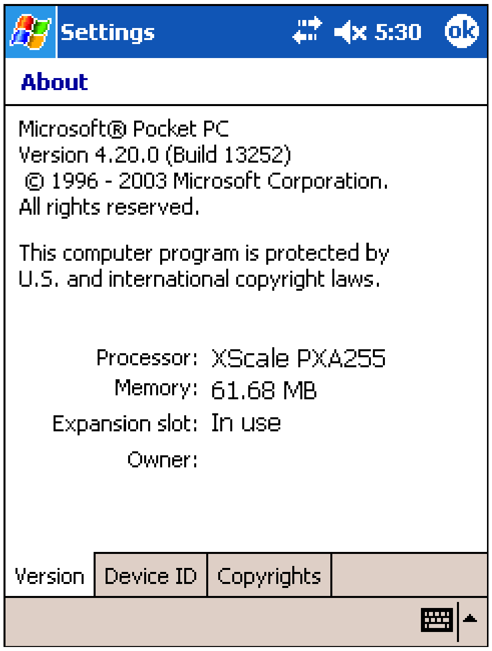
The System tab enables you to verify and sometimes alter system parameters. To access the System tab, go to **Start** > **Settings** > **System** tab. Tap the appropriate icon to open that system setting.



About

The About system setting displays specific information about what is loaded on the terminal. It contains three tabs:

Version tab Displays the information about the software, operating system, and processor of the terminal.



About

Microsoft® Pocket PC
Version 4.20.0 (Build 13252)
© 1996 - 2003 Microsoft Corporation.
All rights reserved.

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

Processor: XScale PXA255
Memory: 61.68 MB
Expansion slot: In use
Owner:

Device ID tab Displays the information the terminal uses to identify itself to other devices. It can be important to know this information if the Dolphin terminal is going to be part of a networked system of devices.

Device name: Displays the system’s default name. This is the name used by ActiveSync.

Description: Displays the description of the device ID.

Copyrights tab Displays important copyright information.

Backlight

The Backlight system setting enables you to customize backlight functionality for the display. For more information, see Adjusting the Backlight on page 4-6.

Certificates

This system setting is designed to manage certificates for 802.11b networks. However, on Dolphin terminals, you manage certificates through Meetinghouse; see Installing Certificates with CertAdd on page 9-41.

ClearType Tuner

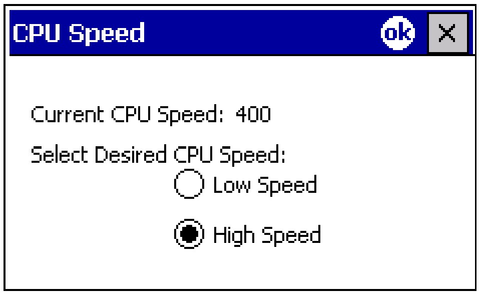
This system setting enables you to adjust the level ClearType font rendering by moving a slider. The sample text displays the setting results immediately. Of course, you must first enable ClearType font rendering to change the appearance of fonts on the screen; see ClearType Tab on page 7-18.

Clock & Alarms

This setting sets the system clock. Appointments, scheduled events, and any function on a schedule runs off this setting. You need to set the time zone and time after each hard reset; see Setting the Time and Date on page 2-9.

CPU Speed

This system setting enables you to see and change the current speed of the Central Processing Unit (CPU).



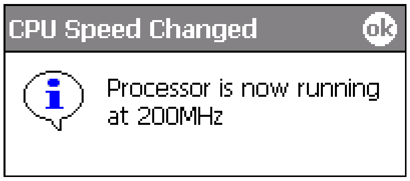
Current CPU Speed: 400

Select Desired CPU Speed:

○ Low Speed

● High Speed

The default is **High Speed** at 400MHz. **Low Speed** is 200MHz. To change the default, select Low Speed and tap **OK**. A message appear confirming the changed and now current CPU speed.



Processor is now running at 200MHz

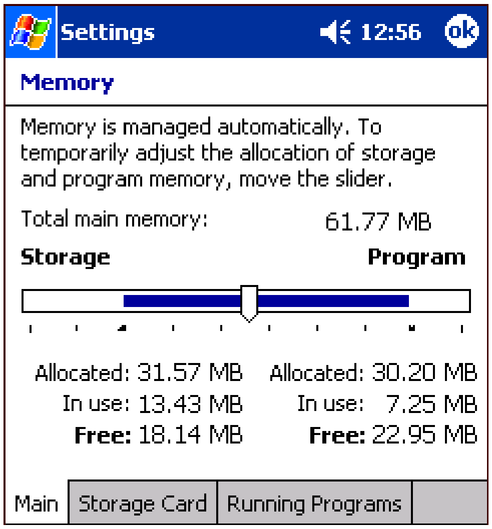
Tap **OK** to save the change.

Memory

The Memory system setting enables you to review and manage both RAM (volatile) and IPSM/Storage Card (non-volatile) memory. Access this system setting whenever you receive system messages about memory.

There are three tabs: Main, Storage Card, and Running Programs.

Main tab — This tab displays current capacity and usage of the 64MB of on-board, volatile RAM memory. This is the memory used for running and storing programs as well as storing program data.



Memory

Memory is managed automatically. To temporarily adjust the allocation of storage and program memory, move the slider.

Total main memory: 61.77 MB

Storage	**Program**
Allocated: 31.57 MB	Allocated: 30.20 MB
In use: 13.43 MB	In use: 7.25 MB
Free: 18.14 MB	**Free:** 22.95 MB

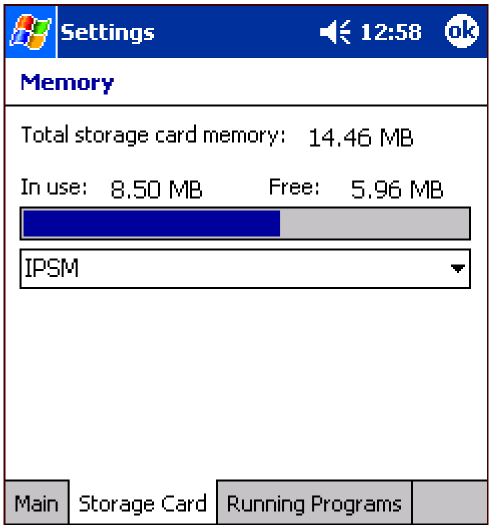
Field	**Description**
Total main memory	The total memory capacity of current RAM memory.
Storage	The part of RAM memory used for storing programs and program data.
Program	The part of RAM memory used to run programs.
Fields Under Storage and Program	
Allocated	Displays the current MB of memory allocated for Storage and Program use.
In use	Displays the total MB of that allocated memory being used in Storage and Program memory functions.
Free	Displays the total MB of memory available for Storage and Programs use.

To Increase/Decrease RAM Memory

To increase Program or Storage memory, tap, hold, and drag the slider towards the kind of memory you want to increase. The three fields adjust automatically; Program memory decrease when you increase Storage memory and vice versa.

Storage Card tab

This tab displays the current capacity and usage statistics of the selected memory type; IPSM or Storage Card. Select the memory type from the drop-down list. IPSM is selected by default.



Total storage card memory: 14.46 MB

In use: 8.50 MB Free: 5.96 MB

IPSM

Total storage card memory	The total MB of memory capacity of the selected memory.
In use	The MB currently being used.
Free	The MB that is still available for use.

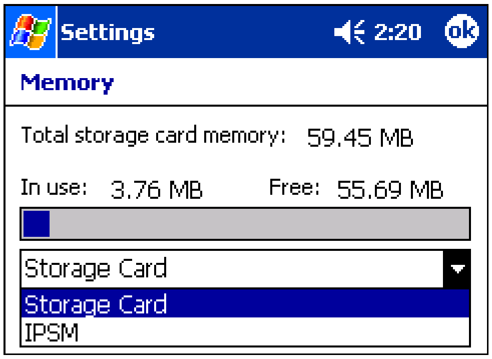
IPSM

Short for Intel Persistent Storage Manager, this is14MB of on-board Flash memory that is non-volatile. Because this memory is non-volatile, data or programs stored in IPSM are not affected when power is removed. Autoinstall programs, for example, are stored in IPSM so that they are always installed at cold-boot startup.

When IPSM is selected in the drop-down list, the Storage Card tab displays the IPSM memory capacity and usage statistics.

Storage Card

You can install additional memory in Dolphin terminals - see Access Door on page 3-5. If a storage card is installed in the terminal, a Storage Card entry appears in the drop-down list.



Total storage card memory: 59.45 MB

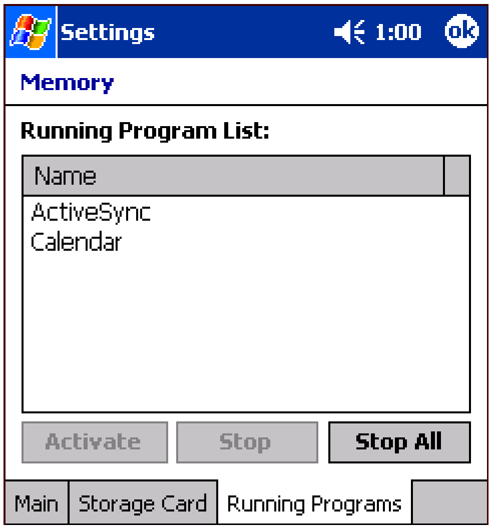
In use: 3.76 MB Free: 55.69 MB

Storage Card

Storage Card
IPSM

Select **Storage Card** and the Storage Card tab displays the current capacity and usage statistics of the installed storage card.

Running Programs tab Displays the software programs currently using Storage memory.



Running Program List:

Name
ActiveSync
Calendar

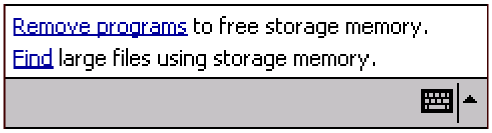
Check this tab when you are receiving out of memory errors or when the mobile computer is running slowly. You can

- Select a program in the list and tap **Stop** to stop it from running (and therefore from using memory), or
- Tap **Stop All** to automatically stop all running programs.

Anytime you stop a running program, it frees up RAM memory. Be advised that, when you stop a program here, any unsaved data in that program is lost. To free up memory without risking data loss, return to the running program, save your data, and close the application.

Links at the Bottom of the Memory Tabs

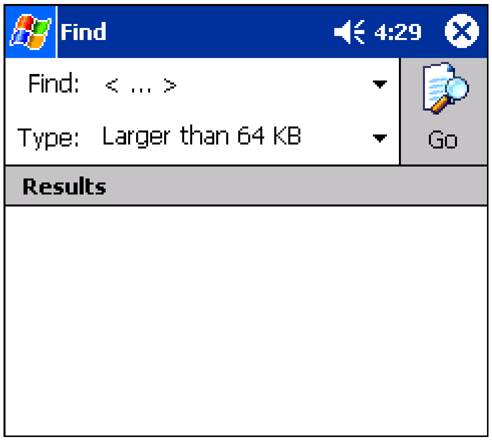
At the bottom of all three Memory tabs are two links:



Remove programs to free storage memory.
Find large files using storage memory.

Remove programs Opens the Remove Programs system setting. For details, see Remove Programs on page 7-15.

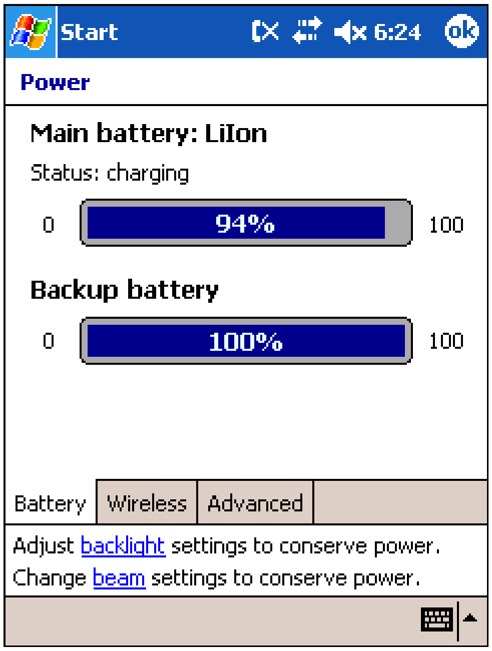
Find Enables you to search for large files using storage memory. It opens the Find screen with **Larger than 64KB** already selected in the **Type** field.



Find: < ... >
Type: Larger than 64 KB

Power

Power system settings contains three tabs: Battery, Wireless, and Advanced.



Main battery: LiIon

Status: charging

0 94% 100

Backup battery

0 100% 100

Adjust backlight settings to conserve power.

Change beam settings to conserve power.

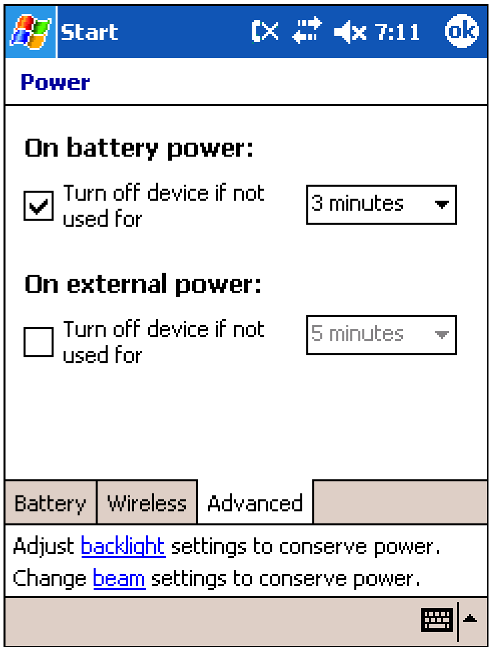
Tab	This tab enables you to …
Battery Tab	Check the remaining charge of both the main and backup batteries. For more information about the terminal’s batteries, see Battery Power on page 3-8.

Tab	This tab enables you to …
Wireless Tab	Determine the power settings for your wireless connection. Select **Wireless signals off…** when you don’t want to use system power to power up the radio(s). Select **Wireless signals on** when you want the radio to use system power to transmit. This is the default settings. The list contains the radio firmware installed in the terminal. The items in the list with a check in the checkbox are the items using system power.

Tab — **This tab enables you to …**

Advanced Tab

Determine power time-outs.



Power

On battery power:

☑ Turn off device if not used for: 3 minutes

On external power:

□ Turn off device if not used for: 5 minutes

Adjust backlight settings to conserve power.

Change beam settings to conserve power.

For **On battery power**, select from the drop-down list, the number of minutes of inactivity you want to pass before the terminal powers off when running on battery power.

For **On external power**, select from the drop-down list, the number of minutes of inactivity you want to pass before the terminal powers off when running on external power.

Options below the tabs

Adjust backlight… opens the Backlight settings so that you can make adjustments to conserve power usage; see Backlight on page 7-7.

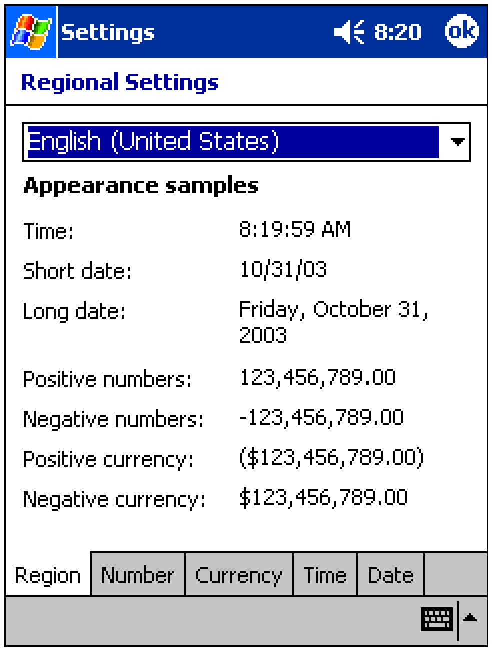
Change beam… opens beam settings so that you can make adjustments to conserve power usage; see Using Infrared on page 8-6. (You would turn off receiving capabilities to conserve power.)

You can also set automatic turn-off times for the terminal to conserve power. When the device is “turned off,” that means that it goes into suspend mode. For more information on suspend mode, see Suspend Mode on page 2-11.

Regional Settings

Regional Settings enables you to customize the appearance and formatting to your geographic region. Specifically, you can customize numbers (number of decimal places allowed, for example), currency (using the $ or € symbol, for example), time, and date. These specifications apply to all screens, including the Today screen.

The Region tab displays an overview of the region selected in the drop-down list at the top.

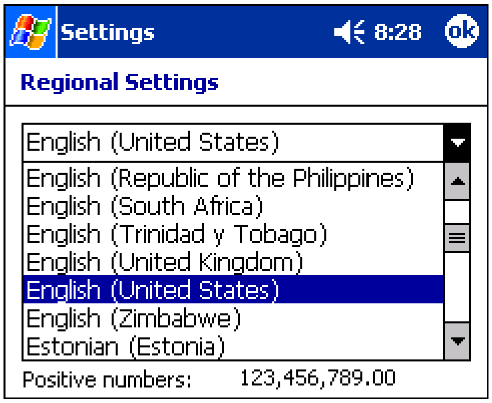


English (United States)

Appearance samples

Time: 8:19:59 AM
Short date: 10/31/03
Long date: Friday, October 31, 2003
Positive numbers: 123,456,789.00
Negative numbers: -123,456,789.00
Positive currency: ($123,456,789.00)
Negative currency: $123,456,789.00

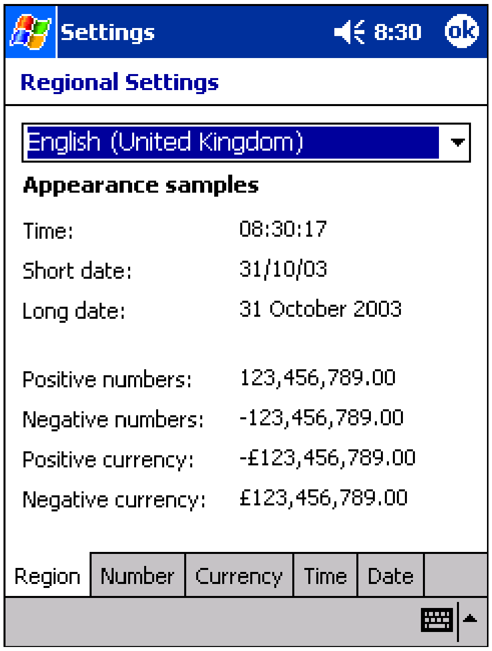
The terminal is loaded with a number of pre-programmed regional settings. Select one from the list.



English (United States)
English (Republic of the Philippines)
English (South Africa)
English (Trinidad y Tobago)
English (United Kingdom)
English (United States)
English (Zimbabwe)
Estonian (Estonia)

Positive numbers: 123,456,789.00

The results appear below.



Regional Settings

English (United Kingdom)

Appearance samples

Time:	08:30:17
Short date:	31/10/03
Long date:	31 October 2003
Positive numbers:	123,456,789.00
Negative numbers:	-123,456,789.00
Positive currency:	-£123,456,789.00
Negative currency:	£123,456,789.00

To see specific settings or change a specific setting, tap on one of the tabs, make the change and tap **OK** to save it.

Remove Programs

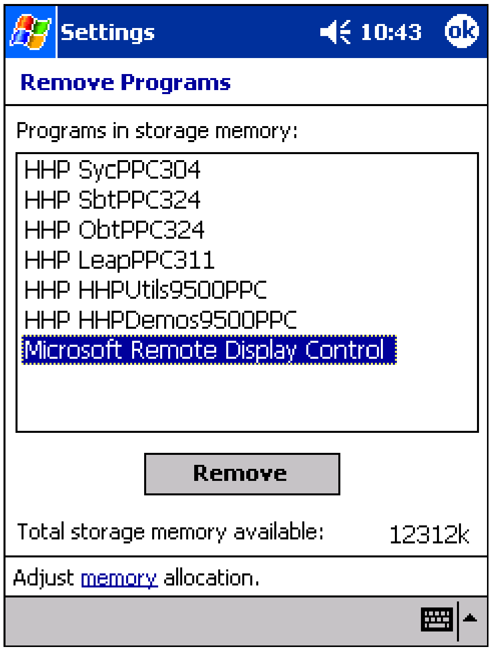
The Remove Programs settings enables you to remove programs installed on the terminal. Use this setting to troubleshoot when you receive messages that the device is out of memory. The programs removed are removed from RAM memory. Any program (usually *.cab or *.dll files) stored in the Autoinstall folder (My Device > IPSM > Autoinstall) will re-install after the next hard reset.

For information about the Autoinstall process, see Autoinstall on page 2-9.

For information about the hard reset process, see Hard Reset (Cold Boot) on page 2-11.

To Remove Programs

1. Tap **Remove Programs**. In the list, select the program you want to remove.



Settings 10:43 ok

Remove Programs

Programs in storage memory:

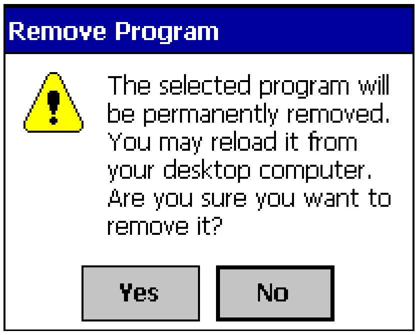
HHP SycPPC304
HHP SbtPPC324
HHP ObtPPC324
HHP LeapPPC311
HHP HHPUtils9500PPC
HHP HHPDemos9500PPC
Microsoft Remote Display Control

Remove

Total storage memory available: 12312k

Adjust memory allocation.

2. Tap **Remove**. The following message appears:



Remove Program

The selected program will be permanently removed. You may reload it from your desktop computer. Are you sure you want to remove it?

Yes No

3. Tap **Yes**. Wait while the program is removed.

4. Verify that the program no longer appears in the list.

Memory

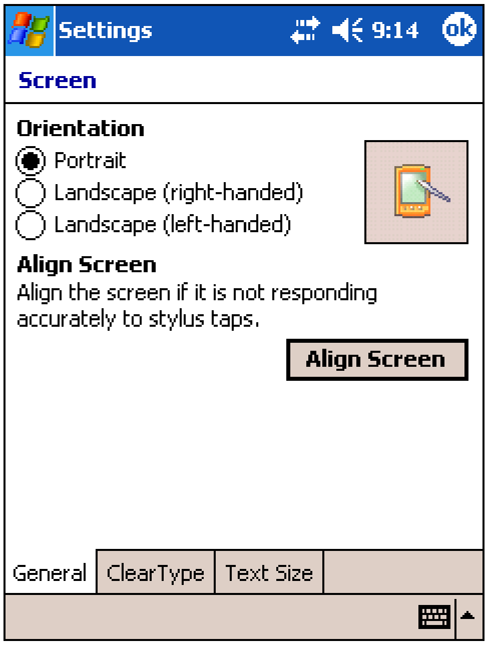
The Remove Programs screen displays the total storage memory available. It adjusts automatically when a program is removed for quick reference. For more detailed memory information, tap **memory** of "Adjust memory allocation" along the bottom margin. It opens the Memory system setting. For information about memory settings, see Memory on page 7-8.

Screen

The Screen system setting contains three tabs: General, Clear Type, and Text Size.

General tab

The Screen system setting opens to the General tab. On this tab, you can changes the screen orientation and align the screen.



Screen

Orientation

● Portrait

○ Landscape (right-handed)

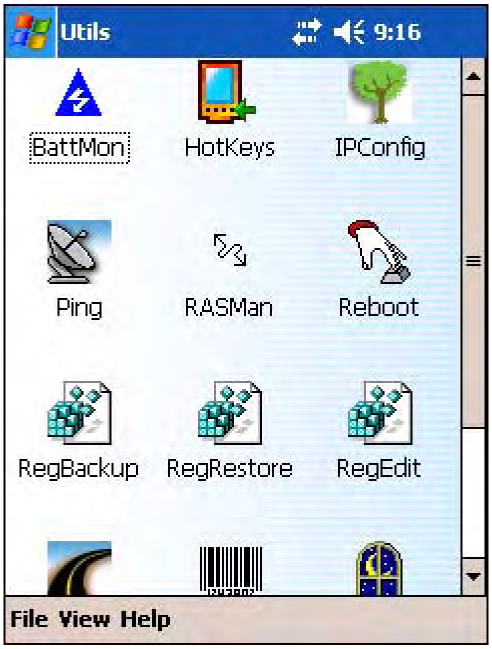
○ Landscape (left-handed)

Align Screen

Align the screen if it is not responding accurately to stylus taps.

The default screen orientation is **Portrait**. You can change the orientation to **Landscape (right-handed)** or **Landscape (left-handed)** depending on which hand you tend to hold the terminal.

Portrait Orientation

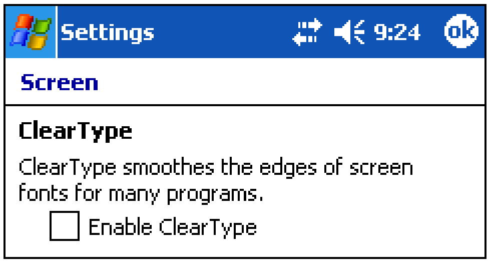


Landscape Orientation - NEED GRAPHIC

To align the screen, tap **Align Screen**, and follow the instructions. See Align the Screen on page 2-7. You would need to re-align the screen if tapping buttons or icons with the stylus no longer seems to work appropriately.

ClearType Tab

The Dolphin 7900 displays support ClearType font rendering. ClearType is a Microsoft technology that dramatically increases the readability of text on LCD displays. To enable ClearType font rendering, select **Enable ClearType** and tap **OK**.



ClearType smoothes the edges of screen fonts for many programs.

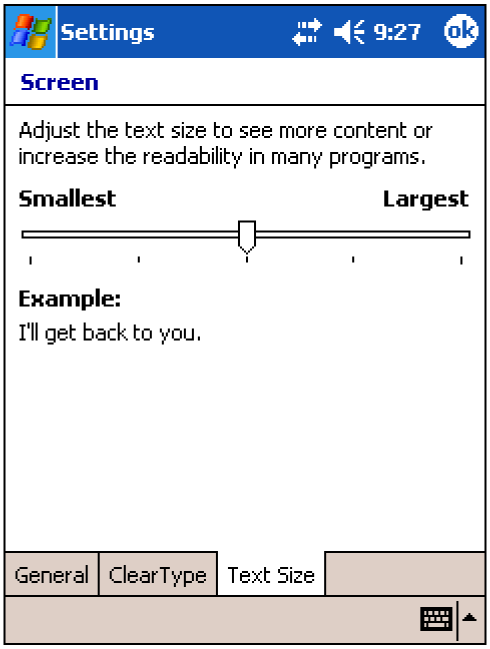
□ Enable ClearType

To adjust the level of ClearType font rendering, use the ClearType Tuner; see ClearType Tuner on page 7-7.

For more information about ClearType font rendering, visit: www.microsoft.com/typography/cleartype/what.htm?fname=%20&fsize=

Text Size Tab

The Text Size tab enables you to perform font scaling within certain views of the Today screen, Contacts, Calendar, Messaging, and Tasks. This means that you can increase or decrease the point size of the font on application windows.



Adjust the text size to see more content or increase the readability in many programs.

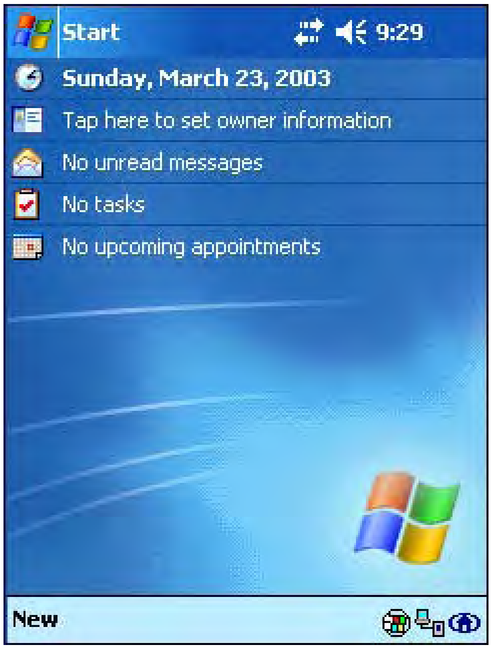
Example:

I'll get back to you.

This is the default font size setting.

To change the font size, move the slider toward Smallest or Largest. The Example text changes to reflect the font change. Tap **OK** to save the new font size setting.

Default Font Size



Start 9:29

Sunday, March 23, 2003

Tap here to set owner information

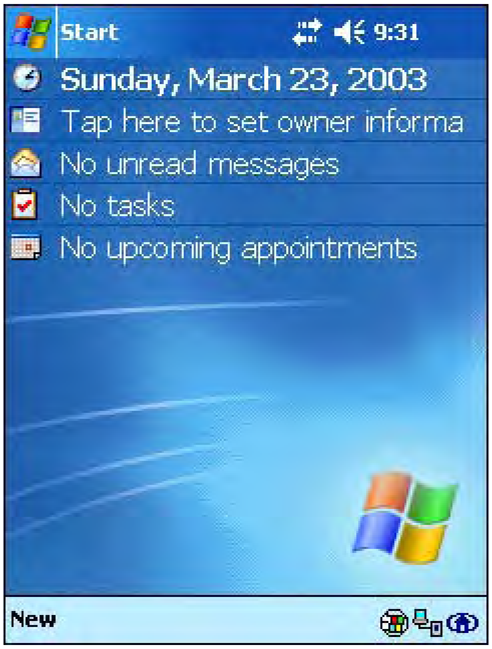
No unread messages

No tasks

No upcoming appointments

New

Largest Font Size



Start 9:31

Sunday, March 23, 2003

Tap here to set owner informa

No unread messages

No tasks

No upcoming appointments

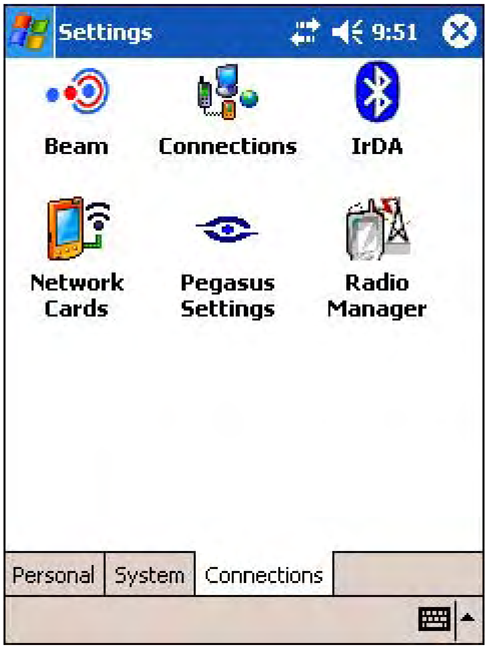
New

uPhone Settings

If you have a GSM/GPRS radio installed on your terminal the uPhone Settings icon appears on the System tab. For details, see uPhone Configuration on page 11-20.

Connections Tab

The Connections tab enables you to manage your network connections.



Icon	**Tapping this icon…**
Beam	Enables you to verify and adjust the infrared settings of the IrDA port; see Using Infrared on page 8-6.
Connections	Enables you to configure network connections. This is the connections manager; see Connections Tab on page 7-20.
Radio Manager	Enables you to power up and power down the radios installed on the terminal; see The Radio Manager on page 4-8.
Network Cards	Enables you to access the Wireless and Network Adapters tabs; see Network Cards **on page 7-35**

Other Icons on the Connections Tab

Other icons appear on this window if your terminal is configured with specific network software, protocols, and/or radios.

HHP WLAN Settings	This icon appears **only** if an 802.11b radio is installed on the terminal. Tapping this icon enables you to configure your 802.11b radio; see Wireless LAN Communications with 802.11b on page 9-1.
IrDA	This icon appears **only** if a Bluetooth radio is installed on the terminal. Tapping this icon enables you to disable or enable the IrDA port; see Verify That the IrDA Port is Enabled on page 8-6.
uPhone GPRS	This icon appears **only** if a GSM/GPRS radio is installed on the terminal. Tapping this icon opens GPRS settings; see GPRS Settings on page 11-26.

Server-Assigned IP Addresses

Please note that all server-assigned IP addresses use Dynamic Host Configuration Protocol (DHCP).

Zero-Config Wi-Fi

Please note that the zero-config Wi-Fi feature of Windows Mobile is **disabled** on Dolphin 7900 series mobile computers.

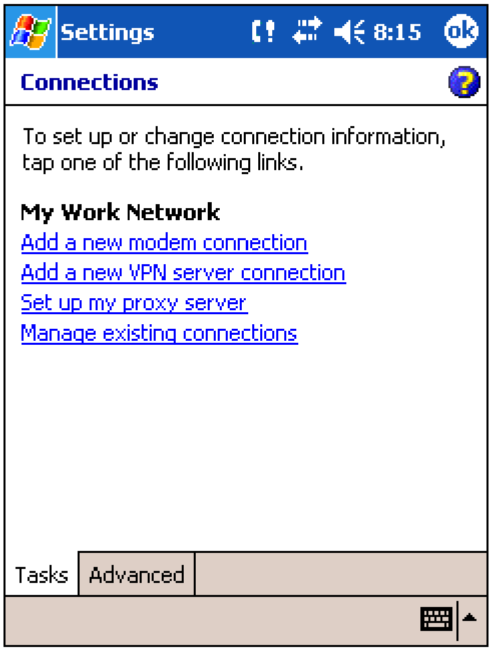
Com Port Assignment Table

The Dolphin 7900 terminal ships with the Com ports assigned as follows:

Com Port	**Assignment**
Com Port 1	Serial port; this is the 17-pin connector on the bottom panel. See Mechanical Connector on page 3-7.
Com Port 2	Bluetooth Module If there is no Bluetooth hardware installed on the terminal, this com port is unassigned.
Com Port 3	Raw Infrared
Com Port 4	Unassigned
Com Port 5	USB virtual serial port
Com Port 6	IrDA, if IrDA is enabled. If IrDA is disabled, this com port becomes available. See Verify That the IrDA Port is Enabled on page 8-6.
Com Ports 7, 8, 9	Unassigned; these are virtual com ports that are available for selection only when connecting to devices that use virtual com ports, such as Bluetooth.

Opening the Connections Manager

To open the connections manager, tap **Connections**. The connection manager opens displaying the Tasks tab.



To set up or change connection information, tap one of the following links.

My Work Network

Add a new modem connection

Add a new VPN server connection

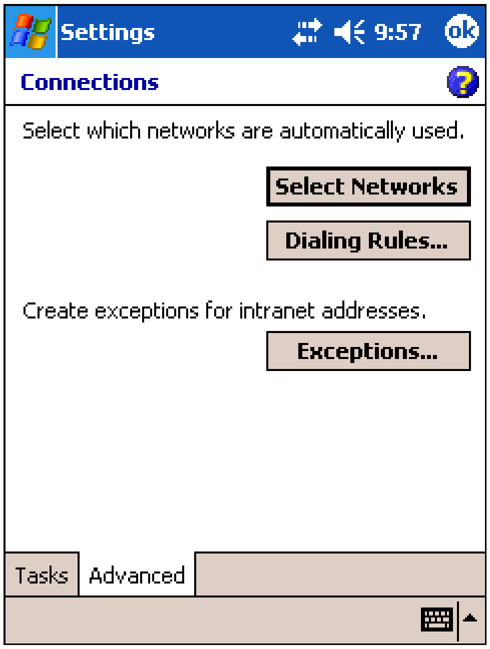
Set up my proxy server

Manage existing connections

The connections manager consists of two tabs: Tasks and Advanced

Task tab — The Task tab enables you to configure and manage your My Work Network settings. Click on the link to setup or manage existing network accounts.

Advanced tab — The Advanced tab enables you to configure and manage network parameters as well as your network cards.

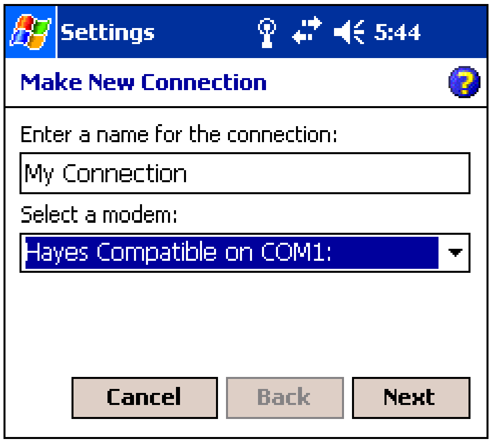


Select which networks are automatically used.

Create exceptions for intranet addresses.

Creating an External Modem Connection to an ISP

1. Obtain the following information from your ISP:
   - ISP dial-up access telephone number,
   - user name,
   - password, and
   - TCP/IP settings.
2. Use a NULL modem cable to connect to an external modem.
3. Tap **Start** > **Settings** > **Connections** tab > **Connections > Task** tab.
4. Tap **Add a new modem connection**. The Make New Connection screen appears.



Make New Connection

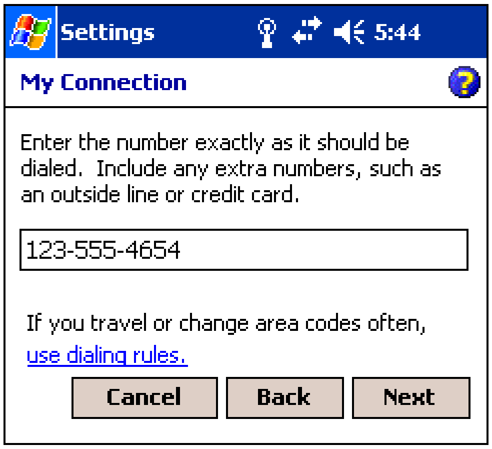
Enter a name for the connection:

My Connection

Select a modem:

Hayes Compatible on COM1:

5. **Enter a name for the connection**, such as "My Connection."
6. In the **Select a modem** list, select the external modem by selecting **Hayes Compatible on COM1**.
7. Tap **Next**. The My Connection screen appears.



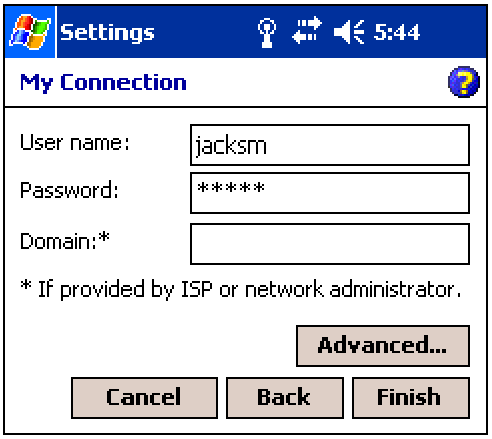
My Connection

Enter the number exactly as it should be dialed. Include any extra numbers, such as an outside line or credit card.

123-555-4654

If you travel or change area codes often, use dialing rules.

8. Enter the number that should be dialed when connecting to your ISP. Include any special digits such as "*" or "#" (see Establishing Dialing Rules on page 7-33). Tap **Next**.



User name: jacksm

Password: *****

Domain:*

* If provided by ISP or network administrator.

9. Now enter any authentication information your ISP requests.

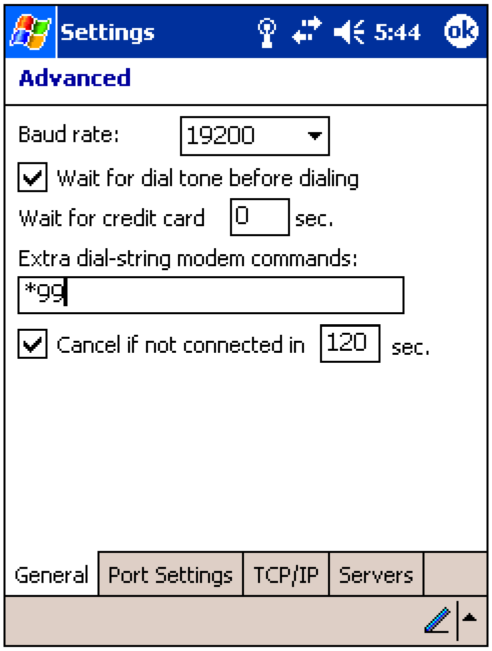
10. You should not need to change any settings in **Advanced** because most ISPs now use a dynamically-assigned addresses. See Advanced Settings on page 7-24.

11. Tap **Finish** to complete this wizard.

Advanced Settings

General Tab

Use the General tab to change the connection speed of your connection. Wait for dial tone before dialing, then wait for credit card, add dial-string modem commands, or cancel call after a set number of seconds.



Baud rate: 19200

☑ Wait for dial tone before dialing

Wait for credit card 0 sec.

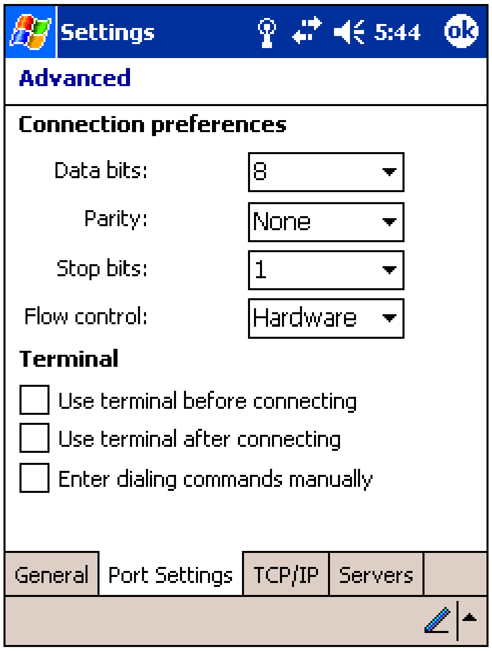
Extra dial-string modem commands:

*99

☑ Cancel if not connected in 120 sec.

Port Settings Tab

The Port Settings tab has options that should be left alone unless indicated otherwise by your ISP.



Advanced

Connection preferences

Data bits: 8

Parity: None

Stop bits: 1

Flow control: Hardware

Terminal

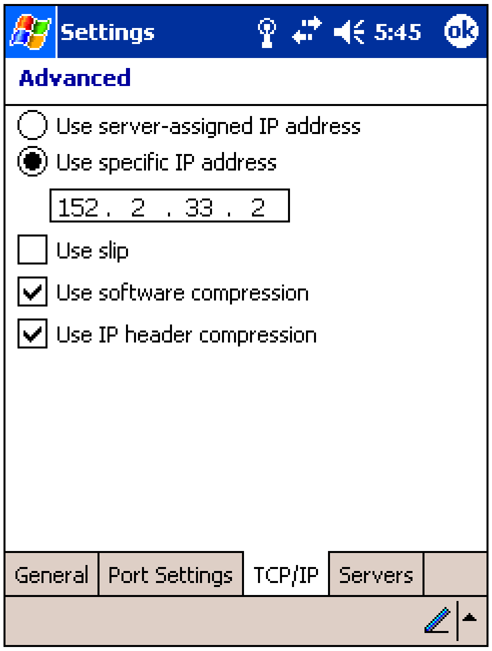
□ Use terminal before connecting

□ Use terminal after connecting

□ Enter dialing commands manually

TCP/IP Tab

If your ISP does not use a dynamically-assigned address, enter that information into the TCP/IP tab.



Advanced

○ Use server-assigned IP address

● Use specific IP address

152 . 2 . 33 . 2

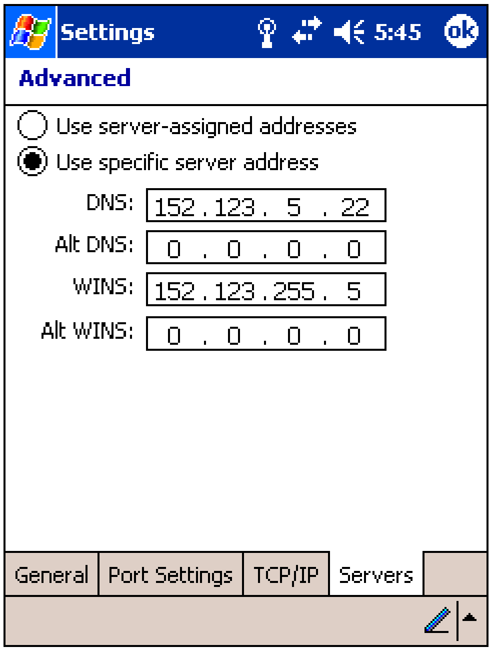
□ Use slip

☑ Use software compression

☑ Use IP header compression

Servers Tab

Finally, if your ISP requires special DNS or WINS information, enter it into the Servers tab.



Settings 5:45 ok

Advanced

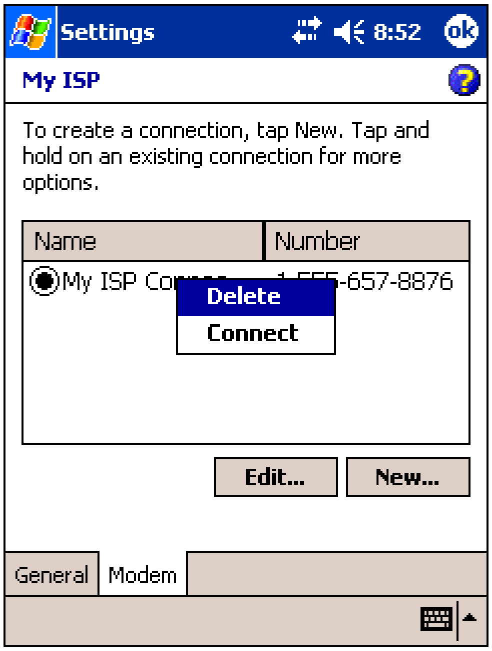
○ Use server-assigned addresses

● Use specific server address

DNS:	152 . 123 . 5 . 22
Alt DNS:	0 . 0 . 0 . 0
WINS:	152 . 123 . 255 . 5
Alt WINS:	0 . 0 . 0 . 0

Connecting to Your ISP

1. Tap **Start** > **Settings** > **Connections** tab > **Connections** to open the connections manager.
2. Tap **Manage existing connections**.



Settings 8:52 ok

My ISP

To create a connection, tap New. Tap and hold on an existing connection for more options.

Name	Number
● My ISP Co…	1-555-657-8876

3. Tap and hold on the applicable dial-up settings and select **Connect**.
(You can delete the connection by selecting Delete.)
4. Your modem will dial-out and attempt to create the connection.

Creating an External Modem Connection to Your Work

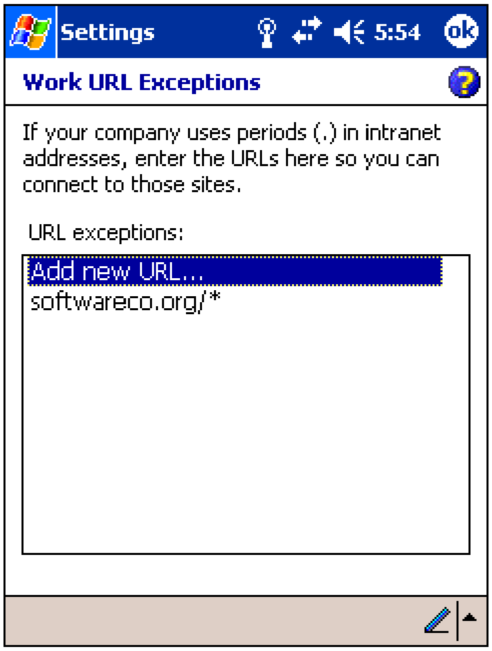
Follow the instructions for Connecting to Your ISP, but select **Add a new modem connection** under **My Work Network**.

Establishing Exceptions for Work URLs

Some companies use periods in their intranet URLs (for example, intranet.companyname.com). If you attempt to connect to one of these URLs, Pocket Internet Explorer will search for the website on the Internet rather than the company's intranet.

To connect to such intranet URLs, they need to be entered as Work URL exceptions in the connections manager.

1. Go to **Start** > **Settings** > **Connections** tab > **Connections** > **Advanced** tab (see page 7-22).
2. Tap **Select Networks**.
3. Tap **Exceptions**. The Work URL Exceptions screen opens.



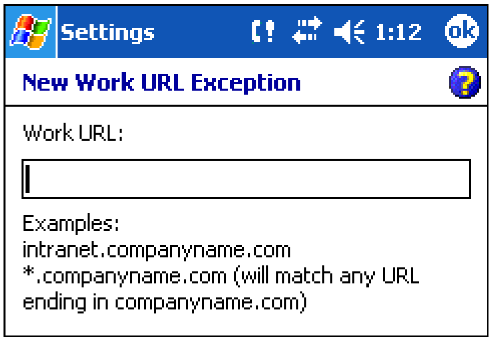
Work URL Exceptions

If your company uses periods (.) in intranet addresses, enter the URLs here so you can connect to those sites.

URL exceptions:

Add new URL...
softwareco.org/*

4. Tap **Add new URL** to add a new exception.



New Work URL Exception

Work URL:

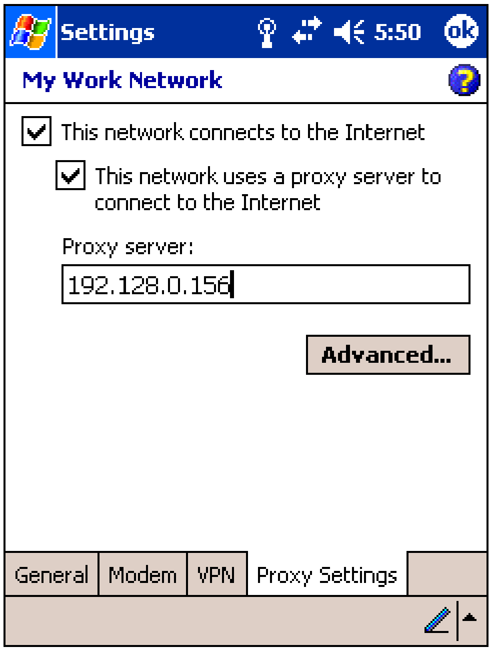
Examples:
intranet.companyname.com
*.companyname.com (will match any URL ending in companyname.com)

5. Enter the **Work URL** and tap **OK**.

Setting up a Proxy Server Connection for Work Connections

If you are connected to your ISP or private network during synchronization, the terminal should download proper proxy settings during synchronization from your PC. If these settings are not on your PC or need to be changed, ask your ISP or network administrator for the proxy sever name, server type, port, type of Socks protocol used, and your user name and password.

1. Go to **Start** > **Settings** > **Connections** tab > **Connections**.
2. Under the My Work Network heading, tap **Set up my proxy server**.



My Work Network

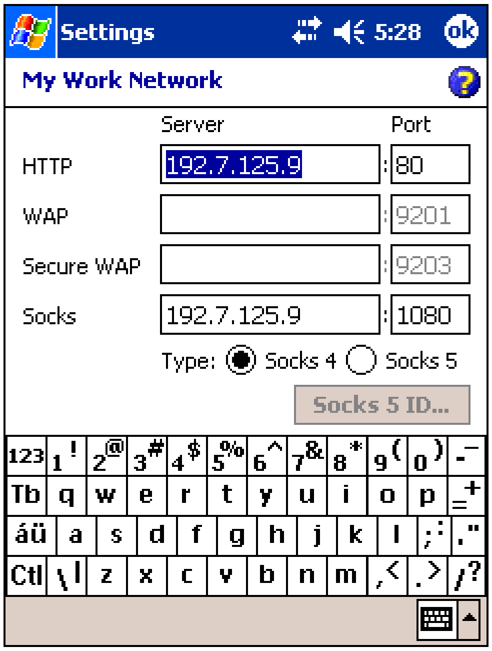
☑ This network connects to the Internet

☑ This network uses a proxy server to connect to the Internet

Proxy server: 192.128.0.156

3. Select **This network connects to the Internet** and **This network uses a proxy server…**
4. In the **Proxy server** field, enter the proxy server name.

- Tap **Advanced** for advanced settings. This information can be provided only by your network administrator.



My Work Network

	Server	Port
HTTP	192.7.125.9	80
WAP		9201
Secure WAP		9203
Socks	192.7.125.9	1080

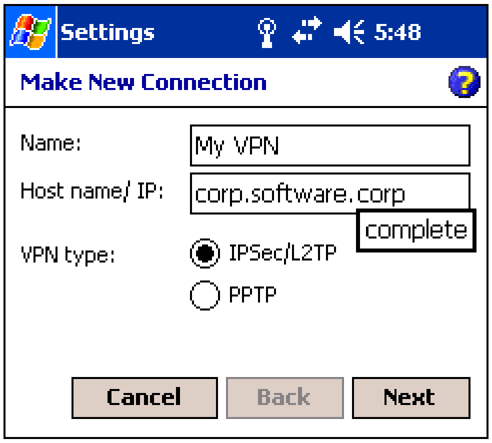
Type: ● Socks 4 ○ Socks 5

5. To change existing settings, under My Work Network, tap **Manage existing connections** and tap the **Proxy** tab.

Setting Up a VPN Connection for Work Connections

A VPN connection helps you securely connect to servers, such as a corporate network, via the Internet. Ask your network administrator for your user name, password, domain name, TCP/IP settings, and host name or IP address of the VPN server.

1. Go to **Start** > **Settings** > **Connections** tab > **Connections**.
2. Under the My Work Network heading, tap **Add a new VPN server connection**.



Make New Connection

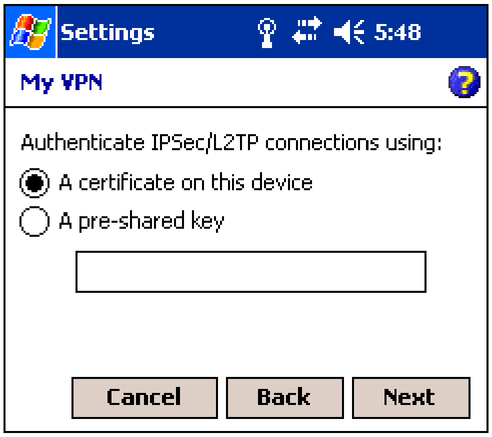
Name: My VPN

Host name/ IP: corp.software.corp

complete

VPN type: ● IPSec/L2TP ○ PPTP

3. Enter the requested information including VPN type and tap **Next**.



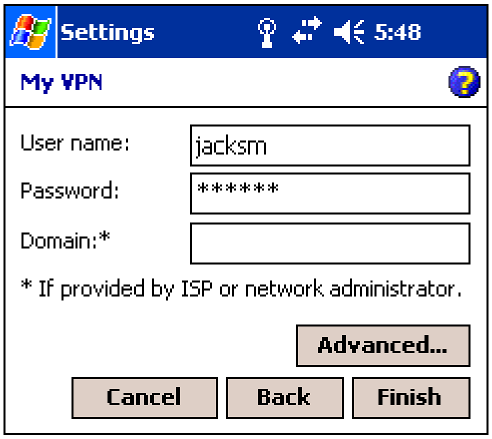
My VPN

Authenticate IPSec/L2TP connections using:

● A certificate on this device

○ A pre-shared key

4. Indicate whether a pre-installed certificate should be used or rather a pre-shared key and tap **Next**.



My VPN

User name: jacksm

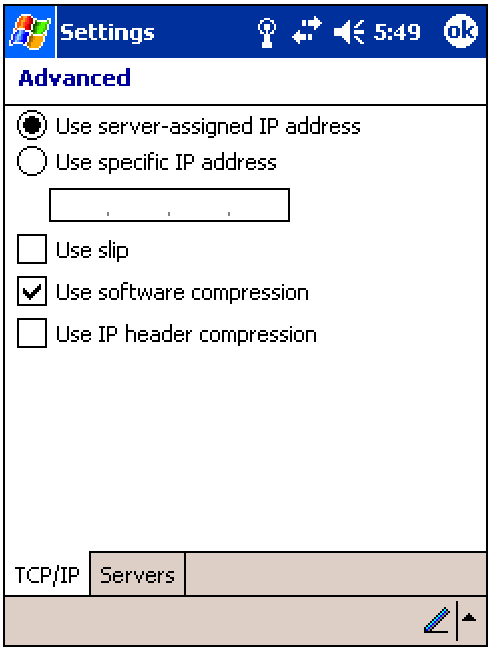
Password: ******

Domain:*

* If provided by ISP or network administrator.

5. Enter your login details. If finished, tap **Finish** to complete VPN setup.

6. Otherwise, tap **Advanced** to access more options.
   - Enter **TCP/IP** settings in the first tab; server-assigned IP addresses use DHCP.



Advanced

● Use server-assigned IP address

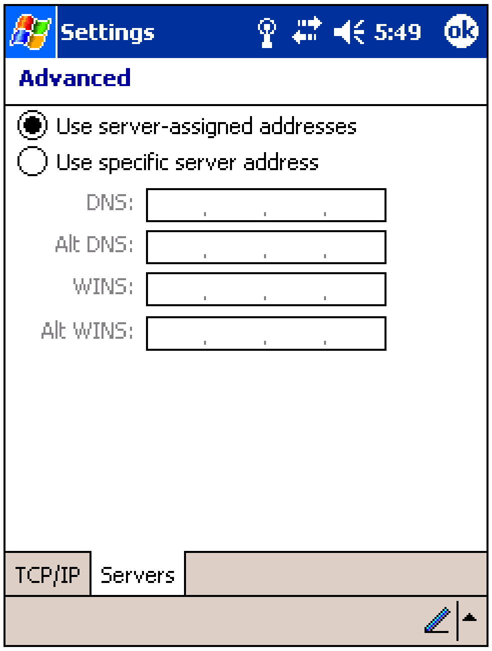
○ Use specific IP address

□ Use slip

☑ Use software compression

□ Use IP header compression

   - Enter Server DNS/WINS information in the **Servers** tab.



Advanced

● Use server-assigned addresses

○ Use specific server address

DNS:

Alt DNS:

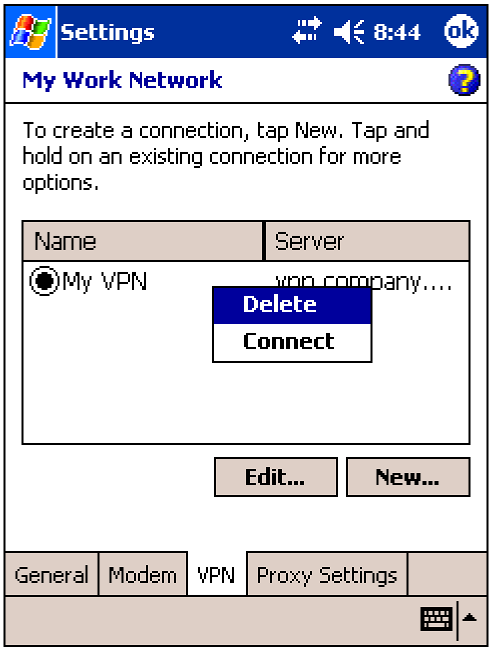
WINS:

Alt WINS:

Connecting to a VPN Server

1. Go to **Start** > **Settings** > **Connections** tab > **Connections**.

2. Select **Edit my VPN servers**.



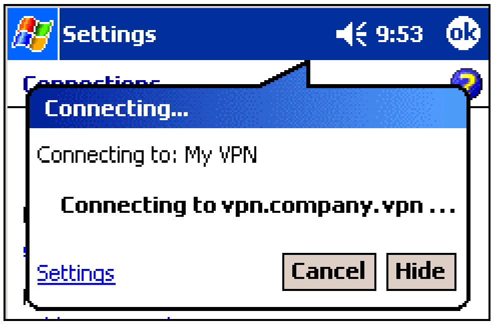
Settings 8:44 ok

My Work Network

To create a connection, tap New. Tap and hold on an existing connection for more options.

Name	Server
● My VPN	vpn.company....

3. Tap and hold on the server, then select **Connect** on the popup menu.
(Note that through this screen you can delete your VPN server connection.)



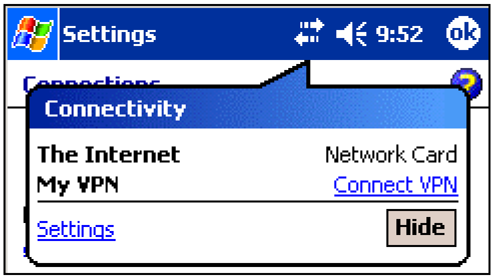
Settings 9:53 ok

Connecting...

Connecting to: My VPN

Connecting to vpn.company.vpn ...

1. Your VPN Server is accessed. When connected, tapping on the ⇄ icon displays the following bubble:



Settings 9:52 ok

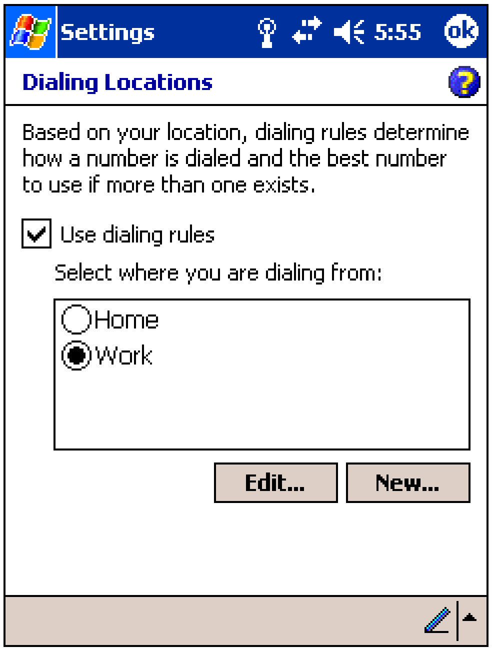
Connectivity

The Internet	Network Card
My VPN	Connect VPN

Establishing Dialing Rules

1. Tap **Start** > **System** > **Connections** tab > **Connections** > **Advanced** tab (see page 7-22).

2. Tap **Select Location**.



Dialing Locations

Based on your location, dialing rules determine how a number is dialed and the best number to use if more than one exists.

☑ Use dialing rules

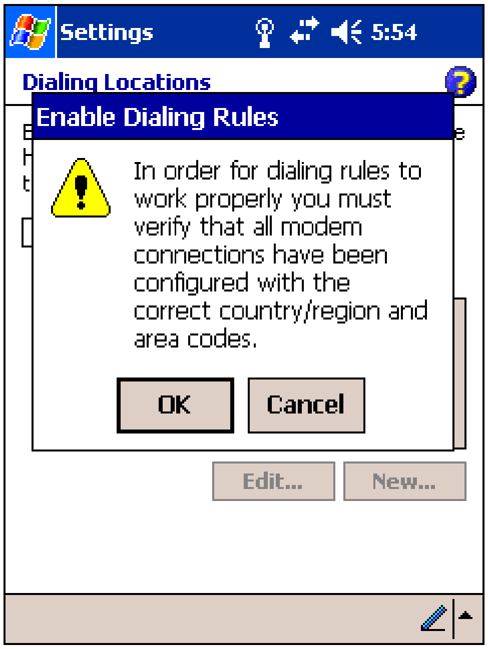
Select where you are dialing from:

○ Home

● Work

3. Select **Use dialing rules**. By default two dialing rules profiles exist: Home and Work.

4. Tap **Edit** to configure either profile.
(You can define your own dialing profile by tapping **New**. A warning appears that your existing modem connections must include the correct country and region area code settings.

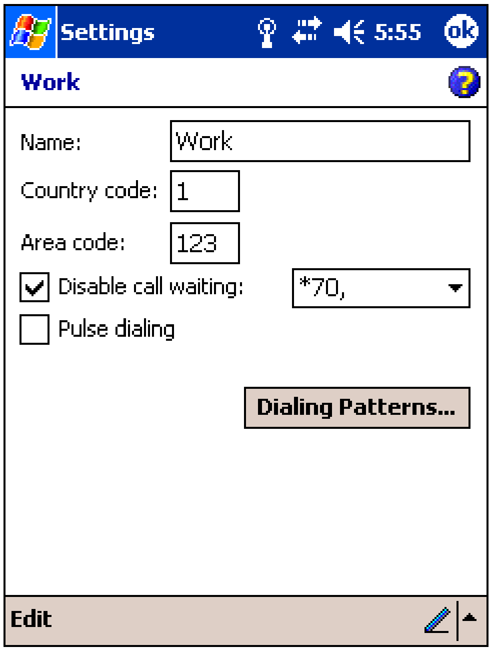


Dialing Locations

Enable Dialing Rules

In order for dialing rules to work properly you must verify that all modem connections have been configured with the correct country/region and area codes.

5. Tap **OK** to confirm. Enter the appropriate information on the next screen.



Name: Work

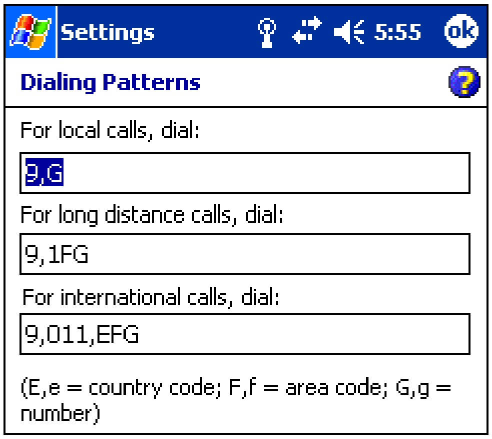
Country code: 1

Area code: 123

☑ Disable call waiting: *70,

□ Pulse dialing

6. Tap **Dialing Patterns** to change how dialing occurs.



For local calls, dial: 9,G

For long distance calls, dial: 9,1FG

For international calls, dial: 9,011,EFG

(E,e = country code; F,f = area code; G,g = number)

7. Following the format of "e" represents country code, "f" represents area code, and "g" represents the number, enter how local, long distance, and international calls should be dialed. Tap **OK** to save your changes.

Creating a Wireless Network Connection

In the Connections Manager, you can access the Wireless tab from **Start** > **Settings** > **Connections** tab > **Network Cards** > **Wireless** tab. However, on the Dolphin 7900, wireless networks need to be configured according to the radio installed in the terminal.

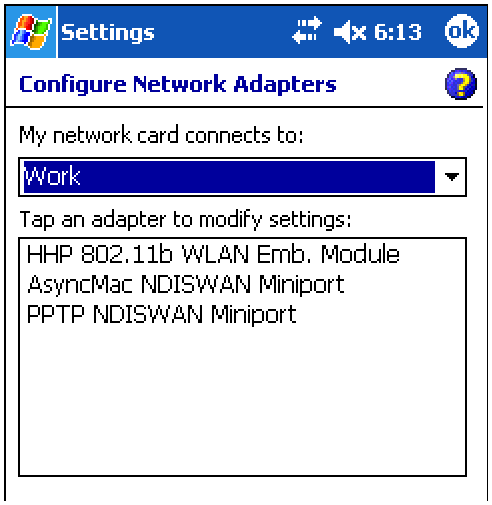
For more information about 802.11b radios, see Wireless LAN Communications with 802.11b on page 9-1.

For more information about Bluetooth radios, see Wireless PAN Communications with Bluetooth on page 10-1.

For more information about GSM/GPRS radios, see Wireless WAN Communications with GSM/GPRS on page 11-1.

Network Cards

To see the network cards installed on your terminal, tap **Start** > **Settings** > **Connections** > **Network Cards > Network Adapters** tab.



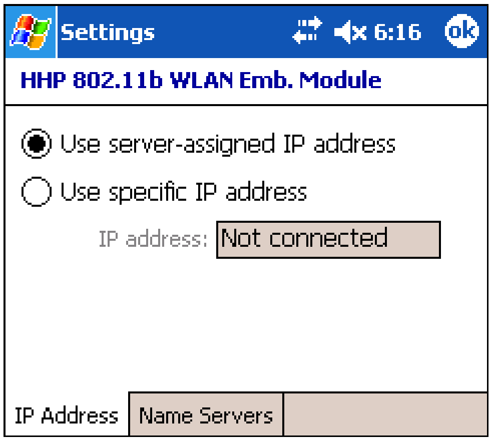
Configure Network Adapters

My network card connects to: Work

Tap an adapter to modify settings:

HHP 802.11b WLAN Emb. Module
AsyncMac NDISWAN Miniport
PPTP NDISWAN Miniport

In the list, tap on an adapter to review its settings. (Server-assigned IP addresses use DHCP.)



HHP 802.11b WLAN Emb. Module

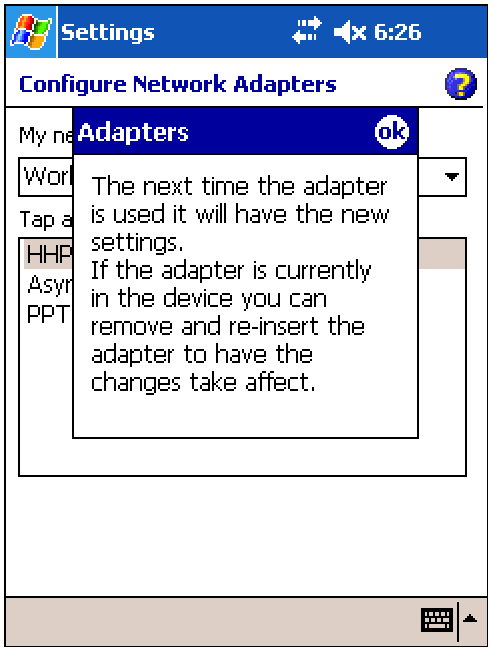
● Use server-assigned IP address

○ Use specific IP address

IP address: Not connected

If you make any changes on these tabs, you must tap **OK** to save the changes, then perform a soft reset to update the registry.

After you tap **OK**, the following message appears:



The next time the adapter is used it will have the new settings.
If the adapter is currently in the device you can remove and re-insert the adapter to have the changes take affect.

Tap **OK** again to save any changes.

For details about performing a soft reset, see Soft Reset (Warm Boot) on page 2-11. During the soft reset, the new registry entries created by the changes can be read by the applications that need them.

⚠ Do **NOT** perform a hard reset (see Hard Reset (Cold Boot) on page 2-11) after modifying an adapter here. Hard resets return the terminal to factory defaults, which means that any modifications are lost.

8

Communications

Overview

You can exchange information between your Dolphin 7900 and other mobile devices, a desktop computer, a network, or the Internet. You have the following connection options:

- Connect to your desktop computer and synchronize via Microsoft ActiveSync v3.7 or higher.
- Use the infrared (IrDA) port to send and receive files between two devices.
- Connect to your ISP.

Help on Connecting

More information on the procedures described here, as well as information on additional procedures, can be found in the following locations:

- ActiveSync Help on the desktop computer. In ActiveSync, click **Help** > **Microsoft ActiveSync Help**.
- See Messaging on page 12-11.
- Online Help. Tap **Start** > **Help** > **View** menu > **All Installed Help > Inbox** or **Connections**.

For more information, go to the Windows Mobile software website at: www.microsoft.com/windowsmobile/products/pocketpc/

Installing Additional Software

In addition to the default programs installed on your terminal when it is first booted up, you can install any program (created for a Windows Mobile device), as long as the terminal has enough memory to store the program and the program has an *.exe, *.cab, or *.dll extension.

The most popular place to find software on the Windows Mobile website: www.microsoft.com/windowsmobile/products/pocketpc/

⚠ *When selecting programs, verify that the program and version of the program are designed for the Windows Mobile 2003 Second Edition and your processor. You can verify your processor by tapping Start > Settings > System tab > About > Version tab. Make a note of the information in the Processor field.*

You can install additional software via:

- ActiveSync - see page 8-4.
- Infrared - see page 8-6.
- The Internet (via wireless radio) - see page 8-10.

Using ActiveSync

Using Microsoft ActiveSync, you can synchronize information in Microsoft Outlook or Microsoft® Exchange Server on your desktop computer with your Dolphin 7900. You can also synchronize this information directly with a Microsoft Exchange server.

Synchronization compares the data on the desktop computer and the terminal and updates both with the most recent data so that the information on both is identical.

You can:

- Update the information in Microsoft Pocket Outlook® on your device by synchronizing it with Microsoft Outlook on your desktop computer.
- Synchronize Microsoft Word and Microsoft Excel files between your device and desktop computer. Your files are automatically converted to the correct format.

The most current version of ActiveSync can be downloaded from www.microsoft.com.

Additional Capabilities

With ActiveSync, you can also:

- Back up and restore your device data.
- Copy (rather than synchronize) files between your device and desktop computer.
- Control when synchronization occurs by selecting a synchronization mode. For example, you can synchronize continually while connected to your desktop computer or only when you choose the synchronize command.
- Select which information types are synchronized and control how much data is synchronized. For example, you can choose how many weeks of past appointments you want synchronized.

Requirements

To synchronize, ActiveSync version 3.7 or higher *must* be installed on both your desktop computer and the Dolphin 7900 terminal. Dolphin 7900 terminals ship with ActiveSync 3.7 already installed. Therefore, you must install ActiveSync 3.7 on your desktop computer from the Microsoft Companion CD that came with your terminal.

To install ActiveSync on your desktop computer, insert the Microsoft Companion CD into the CD-ROM drive of your desktop computer. Click the **yellow arrow**, then **Start Here**, and follow the directions on your screen.

⚠ *When communicating via ActiveSync, your terminal must be connected to the host PC with a peripheral device sold/manufactured by HHP, such as the Dolphin HomeBase, Dolphin Mobile Base, Dolphin Net Base, Dolphin Mobile Charger or other Dolphin 7900 series charging/communication cable. Use of any peripheral not sold/manufactured by HHP may damage your terminal and will void the warranty.*

For more information about communication peripherals, see Dolphin 7900 HomeBase on page 13-1 and Dolphin 7900 Mobile Base on page 14-1.

Setting Up Your Desktop Computer

When installation of ActiveSync is complete on your desktop computer, the ActiveSync Setup Wizard helps you

- connect your terminal to your desktop computer,
- set up a partnership so you can synchronize information, and
- customize your synchronization settings.

Synchronizing from Your Desktop Computer

Because ActiveSync is already installed on the Dolphin 7900 terminal, your first synchronization process begins automatically when you finish setting up your desktop computer in the wizard and your terminal is connected to the host PC.

After your first synchronization, look at Calendar, Contacts, and Tasks on the terminal. Notice that the same information from Microsoft Outlook on your desktop computer is now on the terminal. Simply remove the Dolphin from the communication peripheral and you're ready to use it.

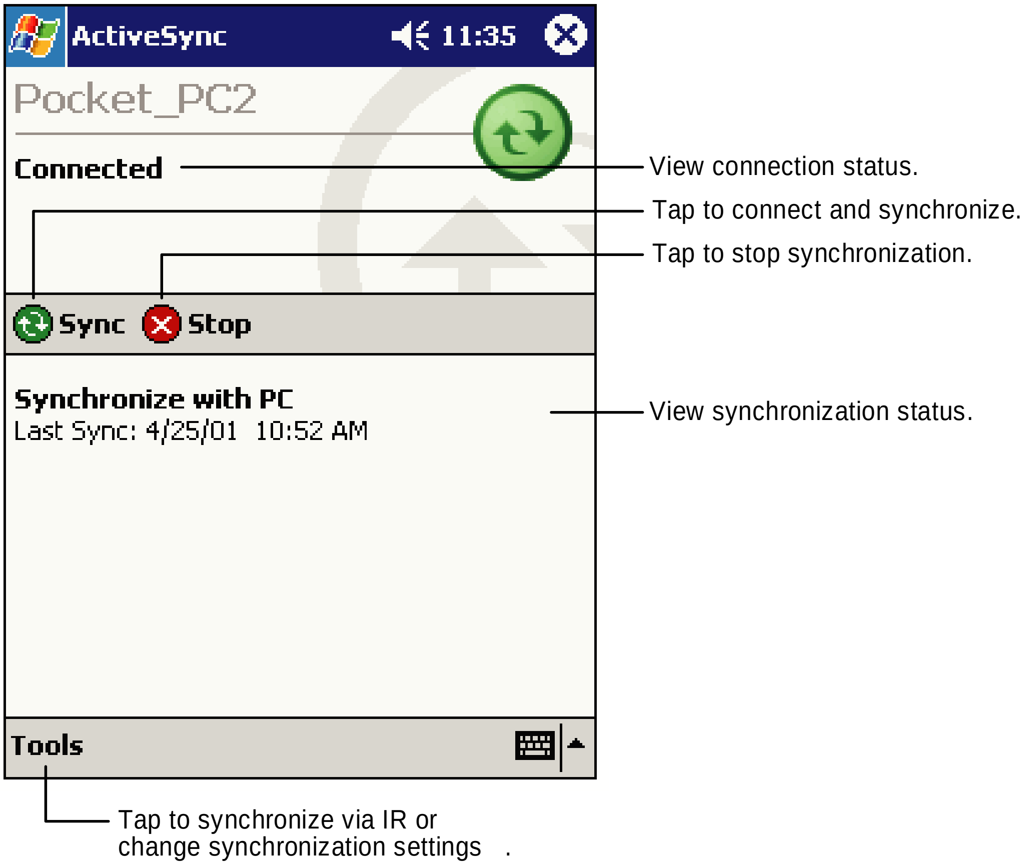
By default, ActiveSync does **not** automatically synchronize all types of information. Use **ActiveSync Options** to specify the types of information you want to synchronize. The synchronization process makes the data (in the information types you select) identical on both your desktop computer and your device.

For more information about using ActiveSync on your desktop computer, open **ActiveSync**, then open **ActiveSync Help**.

Synchronizing from the Terminal

ActiveSync **must** be setup on your desktop computer and the first synchronization process completed *before* you initiate synchronization from the terminal for the first time.

To initiate synchronization the first time, tap **Start** > **ActiveSync**. The synchronization process begins.



Connected

Synchronize with PC
Last Sync: 4/25/01 10:52 AM

View connection status.

Tap to connect and synchronize.

Tap to stop synchronization.

View synchronization status.

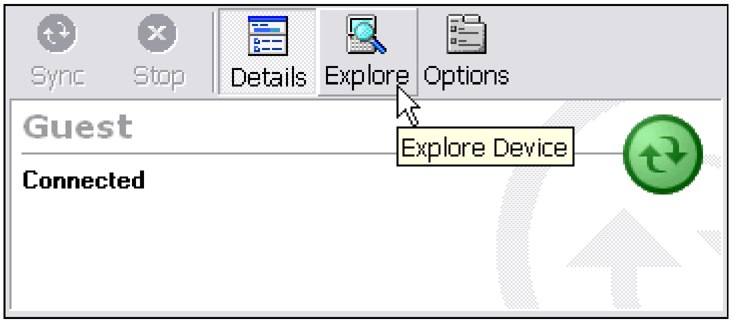
Tap to synchronize via IR or change synchronization settings .

Note: If you have a wireless LAN card, you can synchronize remotely.

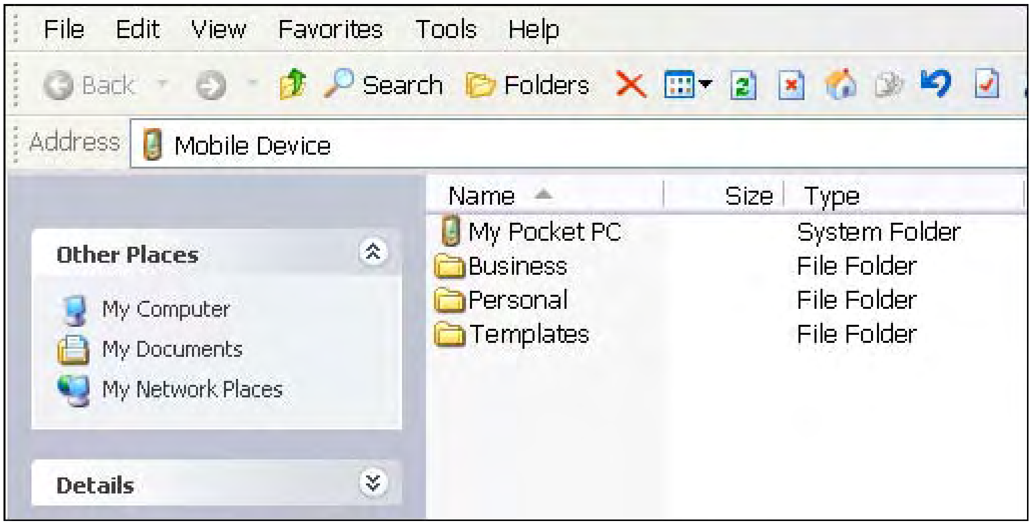
After the first synchronization, when using Dolphin peripherals such as the HomeBase or Mobile Base, synchronization begins automatically whenever a terminal is properly seated in the terminal well. For more information, see Dolphin 7900 HomeBase on page 13-1 or Dolphin 7900 Mobile Base on page 14-1.

Exploring the Terminal from the Desktop Computer

When the terminal and desktop computer are connected, open the main ActiveSync window (on the desktop), and click **Explore**.



The Mobile Device folder opens in Windows Explorer.



The terminal is now treated as a mass storage device, and transferring files is as simple as dragging and dropping or copying and pasting as you would for moving files between folders on your hard drive.

Adding Programs to the Terminal Using ActiveSync

⚠ *When selecting programs, verify that the program and version of the program are designed for Windows Mobile 2003 Second Edition and your processor. You can verify your processor by tapping Start > Settings > System tab > About > Version tab. Make a note of the information in the Processor field.*

Depending on the application, the software must be stored or installed on the host PC.

1. Download the program to your desktop computer from either the Internet or the CD or disk that contains the program. You may see a single *.exe or setup.exe file, a *.cab file, or *.dll. There may also be several versions of files for different device types and processors.
2. Read any installation instructions, Read Me files, or documentation that comes with the program. Many programs provide special installation instructions.
3. Connect the terminal to the desktop computer via an HHP communication peripheral.

If the File is an Installer:

An installer program is one that installs on the PC and the terminal simultaneously; one process installs to both devices.

1. On the PC, double-click the *.exe or *.setup.exe file. The installation wizard begins.
2. Follow the directions on the PC screen. The installation process includes transferring the software to the terminal.

If the File is Not an Installer:

Some programs cannot be installed on PCs because they are designed for terminals. In these cases, the appropriate files must be stored on the host PC, transferred via ActiveSync, and installed on the terminal. You will know the program cannot be installed on the PC if an error message appears when you try to install it stating that the program is valid but designed for a different type of computer.

1. If you cannot find any installation instructions for the program in the Read Me file or documentation, open **ActiveSync** and click **Explore**.*
2. Navigate to the **My Pocket PC** folder and copy the program file or files to the **Program Files** folder on the terminal.
   - If you want the program to be part of the Autoinstall that occurs after every hard reset, place the program file in the **Autoinstall** folder (My Pocket PC > IPSM > Autoinstall).
3. Depending on the program, you may need to open **File Explorer** on the terminal, navigate to the folder where the program is located, and tap on the program file to install it.
   - If you copied the file to the **Autoinstall** folder, you can either tap on the program inside the Autoinstall folder or perform a hard reset and the program will install as part of the regular Autoinstall; see Autoinstall on page 2-9. Remember, a hard reset erases RAM data! For more information, see Hard Reset (Cold Boot) on page 2-11.

After installation on the terminal is complete, tap **Start** > **Programs** and the program and its icon appears on the Programs screen. Tap it to open the program.

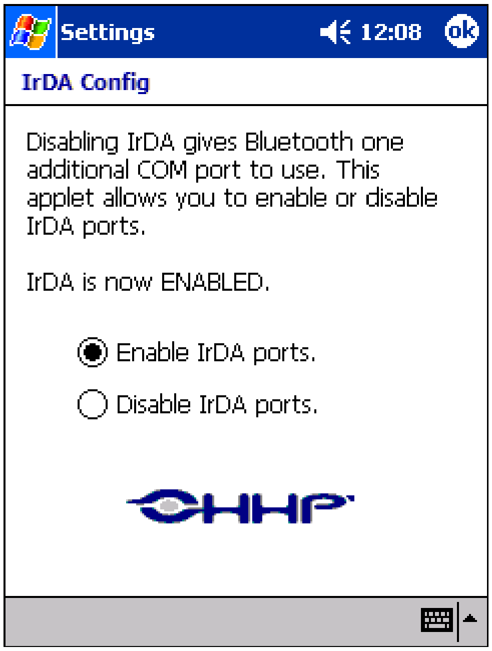
Using Infrared

Dolphin 7900 terminals contain an IrDA port on the top panel (see IrDa Port on page 3-2). Using the IrDA port, you can send and receive data between the terminal and other devices equipped with infrared. This can include, but is not limited to, Windows Mobile information such as Contacts and Tasks, as well as software upgrades.

Verify That the IrDA Port is Enabled

The IrDA port must be enabled to transmit data. By default, the IrDA port is assigned to Com port 6 and is enabled. When a Bluetooth radio is installed, the IrDA port can be disabled to free up a Com port for Bluetooth devices.

To verify that the IrDA port is enabled, tap **Start** > **Settings** > **Connections** tab > **IrDA** **IrDA**.



IrDA Config

Disabling IrDA gives Bluetooth one additional COM port to use. This applet allows you to enable or disable IrDA ports.

IrDA is now ENABLED.

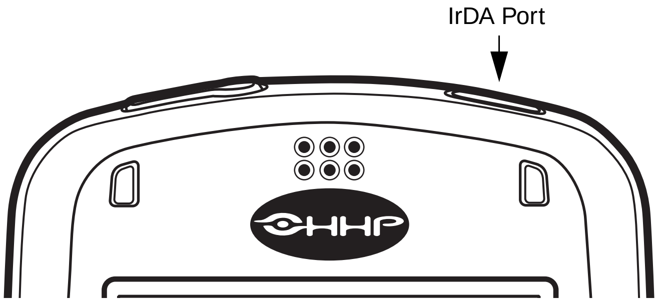
● Enable IrDA ports.

○ Disable IrDA ports.

If **Enable IrDA ports** is selected, then the IrDA port is active.

Note: The IrDA icon appears on the Connections tab **only** if there is a Bluetooth radio installed on the terminal.

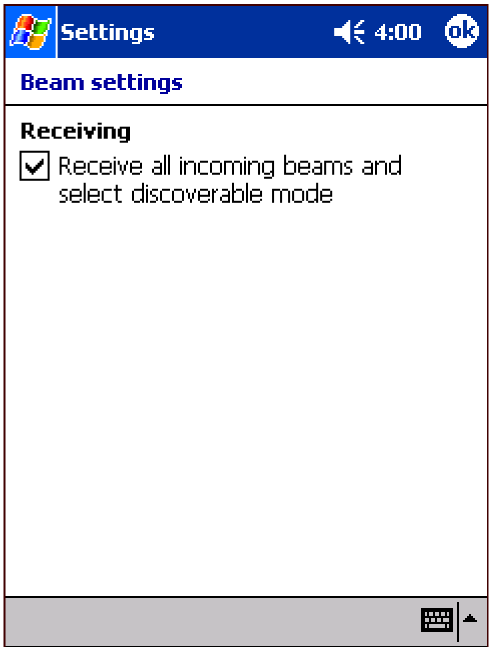
IrDA Port Location on the Terminal



The above graphics shows the left side panel of the Dolphin 7900 terminal. For more information, see IrDA Port on page 3-3.

Verify That Beam Settings Are Set to Receive

The Beam Settings must be set to receive for the terminal to receive data from other infrared devices. To verify, tap **Start** > **Settings** > **Connections** tab > **Beam**. The Beam Settings window should appear as follows:



Beam settings

Receiving

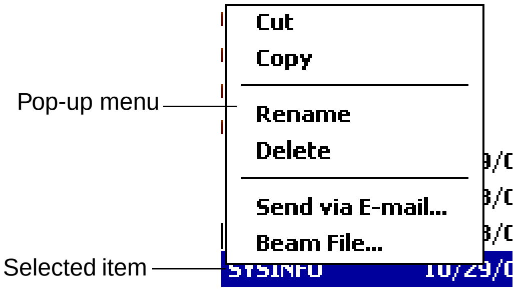
☑ Receive all incoming beams and select discoverable mode

Sending and Receiving Information

To send or receive, the IrDA ports of both devices - whether it's two terminals, or a terminal and a host device - must be aligned with each other and within a close range. The maximum data-transfer speed is 115 Kbps.

Sending

1. Align the IrDA ports.
2. Open the program where you created the item you want to send and locate the item in the list.
   You can also beam files, but not folders, from File Explorer.
3. Tap and hold the item. A pop-up menu appears.



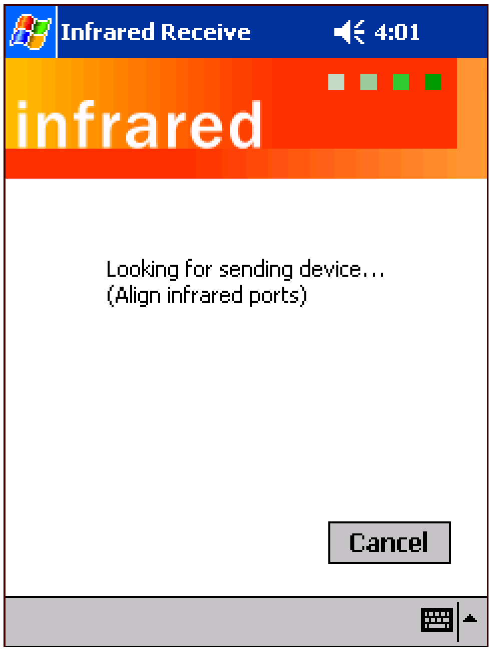
4. Select **Beam File**. The information begins transmitting to the other device.

Receiving

1. Align the IrDA ports.
2. Have the owner of the other device send the information to you.
3. Your terminal automatically begins receiving it.

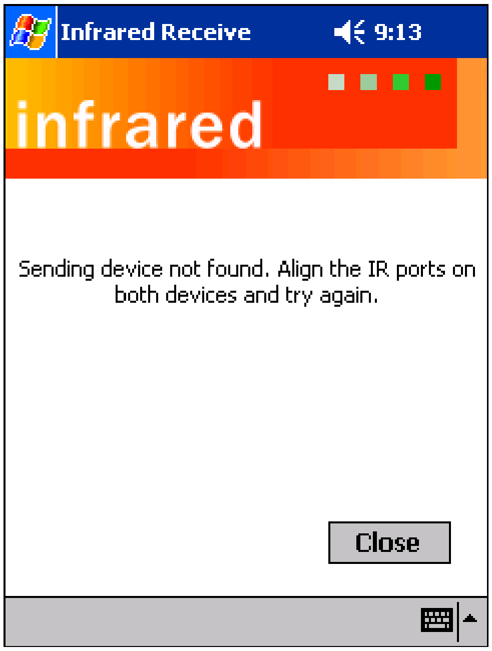
Troubleshooting

If the Beam Settings are not set to receive or you've aligned two IrDA ports and the terminal is still not receiving, go to **Start** > **Programs** > **Infrared Receive**. The terminal searches for the sending device.



Looking for sending device...
(Align infrared ports)

If the terminal cannot find the sending device, the following message appears:



Sending device not found. Align the IR ports on both devices and try again.

Using an ISP

The communication software for creating an ISP connection is already installed on your device. Your service provider should provide the software needed to install other services, such as paging and fax services.

After you are connected, you can send and receive e-mail messages by using Inbox and view web pages using Pocket Internet Explorer. For more information, see Messaging on page 12-11. You can also download software applications from the web.

Adding Programs Directly from the Internet

⚠ *When selecting programs, verify that the program and version of the program are designed for the Windows Mobile 2003 Second Edition and your processor. You can verify your processor by tapping Start > Settings > System tab > About > Version tab. Make a note of the information in the Processor field.*

1. Determine your device and processor type so that you know which version of the software to install. Go to **Start** > **Settings** > **System** tab > **About**. On the **Version** tab, make a note of the information in the **Processor** field.
2. Download the program to your device straight from the Internet using Pocket Internet Explorer. You may see a single *.exe or setup.exe file, or several versions of files for different device types and processors.
3. Read any installation instructions, Read Me files, or documentation that comes with the program. Many programs provide special installation instructions.
4. Tap the file, such as an *.exe file. The installation wizard begins. Follow the directions on the screen.

For more information about working with Pocket Internet Explorer, see Pocket Internet Explorer on page 12-15.

9 Wireless LAN Communications with 802.11b

Overview

Dolphin 7900 terminals are available with an on-board 2.4 GHz 802.11b WLAN (Wireless Local Area Network) radio that uses Direct Sequence Spread Spectrum (DSSS) technology to spread the signal continuously over a wide frequency band at a data rate of up to 11 Mbps. In addition, the open software architecture makes the Dolphin 7900 a complete solution for a variety of wireless mobile data collection applications.

The Dolphin 7900 is interoperable with other 802.11b Wi-Fi-compliant products including Access Points (APs), printers, PCs via PC card adapters and other wireless portable terminals.

Powering Up the 802.11b Radio Driver

When the Dolphin terminal is first initialized, the radio driver for 802.11b is installed. Before using the radio, make sure that the 802.11b radio is powered up. The 802.11b radio must be powered up before you can configure it. For more information, see The Radio Manager on page 4-8.

Configuration Utilities

There are two configuration utilities for the 802.11b radio: 802.11b Settings and 802.11b Wireless Security Supplement.

802.11b Settings Use this configuration utility when you are not using Wired Equivalent Privacy (WEP) or standard WEP (64/128 bit) with no authentication. For more details, see 802.11b Settings on page 9-2.

802.11b Wireless Security Supplement

Use this configuration utility when you are using WEP (beyond the standard), Wi-Fi Protected Access (WPA), and authentication. For details, see 802.11b Wireless Security Supplement on page 9-13.

802.11b Settings

You can access the configuration utility two ways:

1. Tap **Start** > **Settings** > **System** tab > **802.11b Settings**.
   This icon appears on the System tab only if there is an 802.11b radio installed on the terminal.

2. Tap the **Status** icon 📶 in the system tray - see The Status Icon on page 9-12.

The 802.11b Settings utility consists of four tabs: Status, Config, Advanced, and About. Each tab is described in its own section in this chapter.

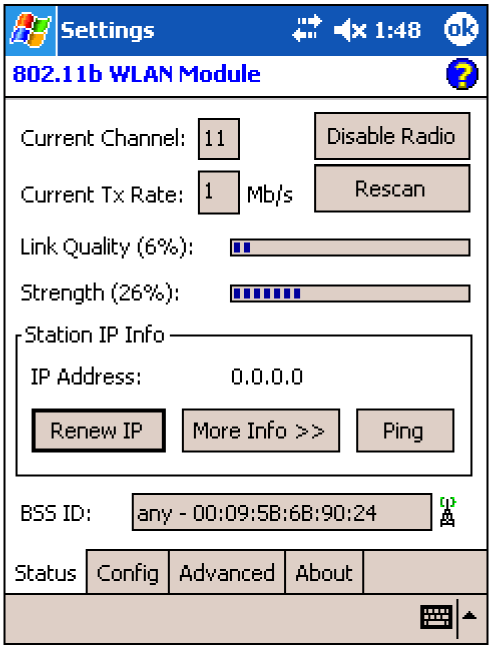
Icons

This configuration utility contains icons that indicate the status of the network.

Icon	This icon means…
📶	Excellent signal strength. Excellent connection.
📡	Poor signal strength. Poor connection.
🚫	Radio disabled. No radio connection.
🖧	Access Point, AP Mode.
💻	Peer Station, Peer-to-Peer Mode.
🔒	WEP enabled. Network needs a WEP Key to connect.
🔓	WEP disabled. Network does not need a WEP Key to connect.
☒	Mismatched WEP Key configuration with your network.
❓	Online help button.

Status Tab

HHP WLAN Settings always opens to the Status tab, which displays the current WLAN settings for 802.11b.



Settings 1:48

802.11b WLAN Module

Current Channel: 11

Current Tx Rate: 1 Mb/s

Link Quality (6%):

Strength (26%):

Station IP Info

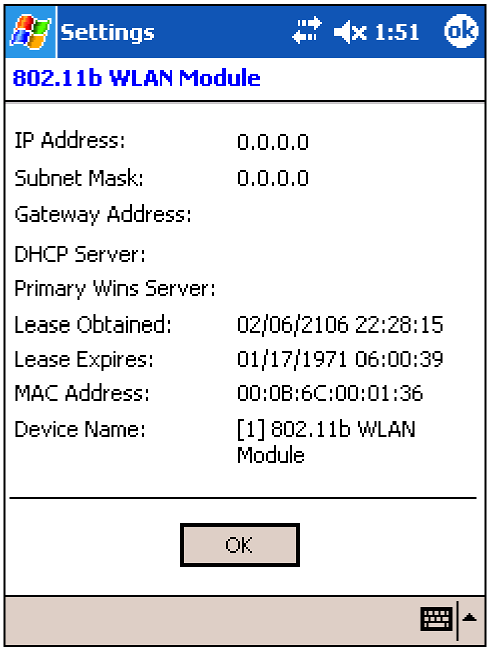
IP Address: 0.0.0.0

BSS ID: any - 00:09:5B:6B:90:24

Field	**Description**
Current Channel	Shows the RF channel currently used by the radio.
Current TX Rate	Shows the current transmit rate. This can be 1 Mbps, 2 Mbps, 5.5 Mbps, or 11 Mbps.
Disable/Enable Radio	Tap this button to disable/enable the radio.
Rescan	Tap this button to start a rescan process to search for an AP with a stronger signal in the network.
Link Quality	Displays the signal to noise ratio.
Strength	Displays the signal strength of the receiver.
IP Address	Displays the IP address of the radio. Verify configuration information with your network administrator.
Renew IP	Tap this button to reapply IP the address from the DHCP server when automatic DHCP is enabled.
State	Displays the Network Name and the MAC address of: - the access point the radio is associated with in AP mode, or - the creator of IBSS into which the radio is joined in peer-to-peer (Ad-Hoc) mode. After an SSID is chosen, this field name changes to “IBSS ID.”

Field **Description**

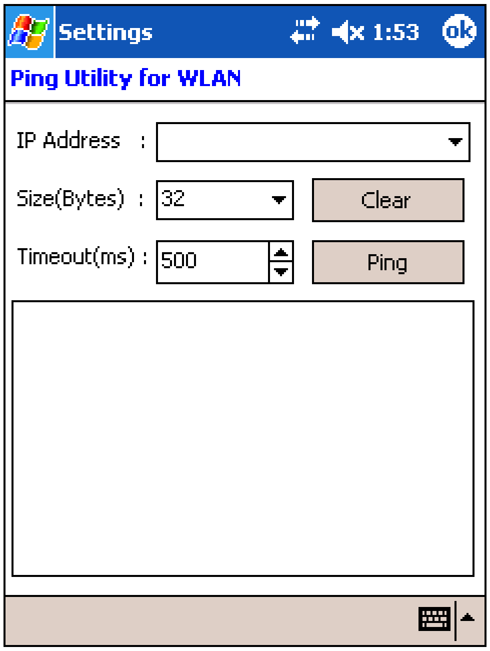
More Info Tap this button to display detailed TCP/IP information as shown in the following screen:



802.11b WLAN Module

IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0
Gateway Address:
DHCP Server:
Primary Wins Server:
Lease Obtained: 02/06/2106 22:28:15
Lease Expires: 01/17/1971 06:00:39
MAC Address: 00:0B:6C:00:01:36
Device Name: [1] 802.11b WLAN Module

Ping Tap this button to open the Ping Utility for WLAN.



Ping Utility for WLAN

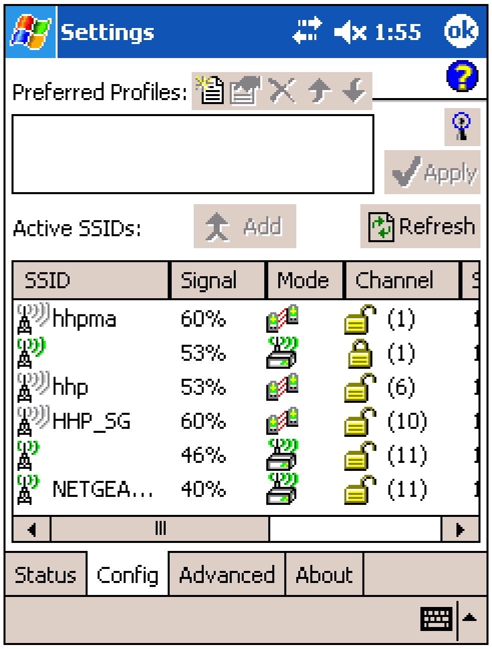
IP Address :
Size(Bytes) : 32
Timeout(ms) : 500

Field	Description
IP Address	Displays the current IP address. You can enter another IP address to ping.
Size (Bytes)	Displays the current bytes size; 32 is the default. You can select up to 8192 from the drop-down list.

Field	Description
Timeout (ms)	Displays the current timeout; 500 is the default. Increase or decrease it by tapping the up and down arrow buttons.
Clear	Tap this button to clear IP Address input and the ping statistics field.
Ping	Tap this button to ping the IP address entered in the input field.
Ping Statistics	This section lists the pinging IP address and the pinging results.

Config Tab

The Config tab provides a list of all access points and peer stations in range. Its configuration tool enables you to create and edit SSID profiles for access points that you want your station to associate with.



SSID	Signal	Mode	Channel
hhpma	60%		(1)
	53%		(1)
hhp	53%		(6)
HHP_SG	60%		(10)
	46%		(11)
NETGEA...	40%		(11)

Preferred Profiles

This section displays a list of preferred profiles for access points (AP) in the network created by the user, or added from the Active SSIDs table. When turned on, the radio searches for the APs in the exact order shown in the list of profiles. This section is blank after the initial installation and each hard reset. It will remain blank if there no automatic association preference selected.

This section contains several icons that enable you to add and configure APs.

Icon	Name	Description
🗎	New	This button is always active. Tap it to create a new profile on a series of screens; for instructions, see To Create a New Profile on page 9-7.

The following buttons activate only when an Active SSID in the Preferred Profile list is selected.

Icon	Name	Description
📝	Edit	Tap this button to open the configuration screens for the selected SSID.
✕	Delete	Tap this button to delete the selected SSID from the Preferred Profile list.
⬆	Up	Tap this button to move the selected SSID up one place in the Preferred Profile list.

Icon	Name	Description
↓	**Down**	Tap this button to move the selected SSID down one place in the Preferred Profile list. Remember that the terminal accesses the SSIDs in this list in the exact order that they appear; moving an SSID up or down in the list determines the order of contact.

Active SSIDs

The Active SSIDs table lists all access points or peer stations (creator of IBSS) in the vicinity of the host. It displays only those SSIDs that accept broadcast associations.

Each record displays information in the following six columns (The screen may not display all the fields in the following table. Use horizontal scroll bar to view all):

Column	This column displays…
SSID	The Network Name of the access point or peer station. An icon with signal strength 📶 is also shown.
Signal	Strength in percentage for the selected SSID.
Mode	An icon indicates an access point or a peer station .
Channel	The channel it uses and the WEP method it applies, if any. The icon 🔒 stands for WEP Key-On, and 🔓 for WEP Key-Off.
SupRate	Supported data rate of the access point or the peer station.
BSSID (MAC Addr)	BSSID or MAC Address of the access point or the peer station.

Add ↑ Add

Tap this button to add an Active SSID to the Preferred Profiles list. Select and active SSID in the list, tap **Add**, and the profile moves to the Preferred Profiles list.

Apply

Tap **Apply** to associate your station with a selected SSID. The SSID selected can be in the Preferred Profile or Active SSIDs lists. When applied, the Status tab opens displaying the status of the wireless connection. If the association fails, a search for another AP in the Preferred Profile list automatically takes place, and the radio attempts to associate with the station, in order of preference.

Refresh

Tap **Refresh** to start a new search for all available access points or peer stations in the vicinity.

To Add an Active SSID to the Preferred Profile Table

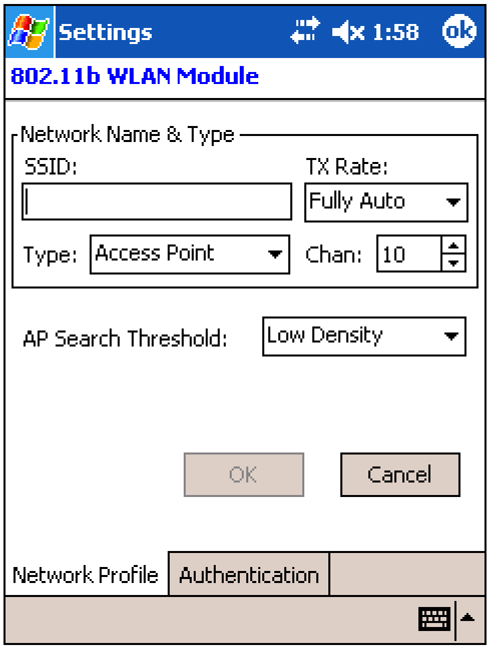
An SSID needs to be in the Preferred Profile list to be edited.

1. Select an SSID in the Active SSID list and tap **Add**. If the SSID has the WEP Key turned on, the Settings window displays and prompts you to enter the WEP Method, Encryption Key, and Key ID.
2. Now, you need to configure its profile.
3. In the Preferred Profile list, select the SSID and tap **Edit** ; see To Create a New Profile on page 9-7.
4. When configuration is complete, tap **OK**. The SSID and its profile are added into the Preferred Profiles list. If adding an SSID with the WEP Key turned off, the Settings window does not display and the SSID is added directly to the Preferred Profile table.

To Create a New Profile

In the Preferred Profiles section, tap the **New** button . A screen opens with two tabs windows: Network Profile and Authentication.

Network Profile Tab



802.11b WLAN Module

Network Name & Type

SSID:

TX Rate: Fully Auto

Type: Access Point

Chan: 10

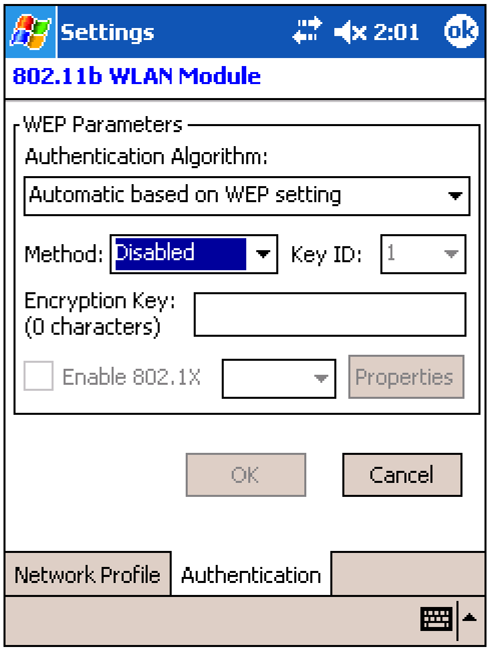
AP Search Threshold: Low Density

Field	Description
Network Name &Type	
SSID	Enter an SSID, which is the Network Name. Check with your network administrator for Network Name (SSID).
TX Rate	Choose the transmit rate from the drop-down list - 1MB, 2 MB, Auto 1/2 MB, 5.5 MB, 11 MB, or Fully Auto. The transmit rate is set to Fully Auto by default.
Type	From the drop-down list, select **Peer-to-Peer** – This mode used for communication between two (or more) radio stations (cards) without an access point. **Access Point** (AP) – This mode is also called “Infrastructure” mode. In most cases, no con
Chan	Scroll to select a channel for communication.
AP Search Threshold	Select **Low Density** (default), **Medium Density**, or **High Density** from the drop-down list and tap **OK**. AP search thresholds are used for wireless client roaming between APs. In general, the higher the density selected here, the easier your WLAN card roams between APs with the same SSID in the same network. Roaming also depends on the relative signal strength of the AP.
OK	Tap this button to save the profile or changes to the profile.
Cancel	Tap this button to close the window without saving or modifying the profile.

Note: The SSID, Type, TX Rate, and Channel fields are unchangeable in Access Point mode, whereas TX Rate and Channel fields can be changed in Peer-to-Peer mode.

Authentication Tab

On the Authentication tab, you configure the WEP encryption key for secure wireless communication.



802.11b WLAN Module

WEP Parameters

Authentication Algorithm: Automatic based on WEP setting

Method: Disabled

Key ID: 1

Encryption Key: (0 characters)

□ Enable 802.1X

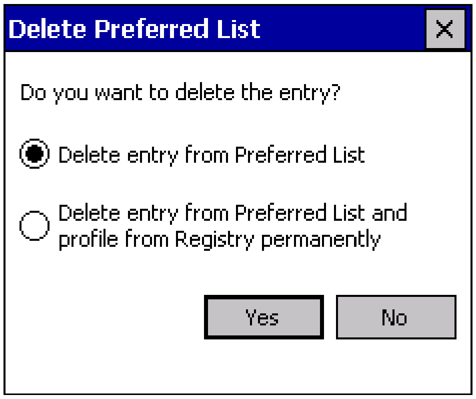
To use WEP, the encryption key must be configured as part of the profile before connecting. For more information about configuring a profile, see To Create a New Profile on page 9-7.

Field	Description
***Authentication Algorithm**	This drop-down list is active and configurable **only** when the WEP Key is enabled for the selected SSID profile. If this drop-down list is active, select one of the following options: **Automatic based on WEP setting** – The algorithm automatically matches the AP's setting. This is the default selection. **WECA Compliant (always use Open)** – The algorithm should match the AP’s setting for "Open." **Must use Shared with WEP** – The algorithm should match the AP's setting for "Shared."
Method	The options in this drop-down list determine what characters can be used to create the WEP encryption key. Select one of the following five: **Disabled** – WEP Key is off **64 bit (HEX)** – You can use up to 10 characters in Hexadecimal in the Encryption Key field **64 bit (ASCII)** – You can use up to 5 characters in ASCII in the Encryption Key field **128 bit (HEX)** – You can use up to 26 characters in Hexadecimal in the Encryption Key field **128 bit (ASCII)** – You can use up to 13 characters in ASCII in the Encryption Key field HEX – Hexadecimal is a set of 16 characters from 0-9 and from A(a)-F(f). ASCII – ASCII means any printable ASCII character can be typed.
Key ID	Choose from the available Key IDs: **1** (Default), **2**, **3**, or **4**. Check with your network administrator for the WEP Key and Key ID you need to use for your network.
Encryption Key	Type in the encryption key for your wireless connection. The format allowed in this field depends on the character set and format selected in the Method field.

Field	Description
***Enable 802.1X**	This option and drop-down list is active **only** when the WEP Key is enabled. Select this option if access to the network needs group authentication, then select the 802.1X security standard - **PEAP** or **TLS** - from the drop-down list.
***Properties**	Tap the Properties button to choose the certificate that applies. Accessing 802.1x networks require personal certificates for authentication.
***Please note that 802.11b Settings does not support authentication; therefore, these fields are not active. If you are using authentication in your wireless 802.11b connection, you must configure that connection in the 802.11b Wireless Security Supplement. For more information, see 802.11b Wireless Security Supplement on page 9-13.**	
OK	Tap this button to save the profile or changes to the profile.
Cancel	Tap this button to close the window without saving or modifying the profile.

To Delete a Profile

Profiles may be deleted either from the Preferred List or from the Preferred List and Registry. To delete a profile, select (highlight) a profile and tap the **Delete** button and the following screen displays:



Delete Preferred List

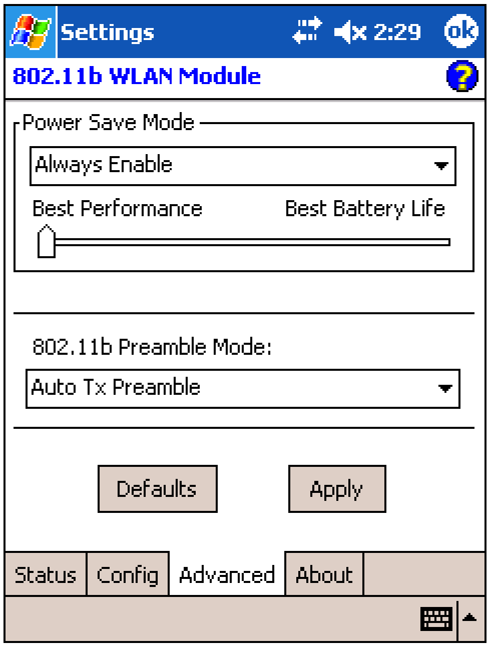
Do you want to delete the entry?

● Delete entry from Preferred List

○ Delete entry from Preferred List and profile from Registry permanently

From the pop-up window select the option of your choice and tap **Yes** to confirm or **No** to cancel.

Advanced Tab



Settings 2:29

802.11b WLAN Module

Power Save Mode: Always Enable

802.11b Preamble Mode: Auto Tx Preamble

Field **Description**

Power Save Mode This drop-down list determines the settings for Power Save Mode.

Disable – Disables the Power Save mode.

Always Enable – Enables Power Save mode. This is the default setting.

Auto Enable – Automatically enables the Power Save mode when the terminal is running on battery power and automatically disables Power Save mode when the terminal is running on external power.

Slider The slider is active only if Power Save Mode is enabled. Move the slider between Best Performance and Best Battery Life. The setting here modulates Power Save Mode to achieve maximum performance and maximum battery life.

Preamble Mode A preamble consists of a Synchronization (Sync) field and a 16-bit Start Frame Delimiter (SFD) field.

Long TX Preamble – Where Sync field consists of 128 bits.

Short TX Preamble – Where Sync field consists of 56 bits.

Auto TX Preamble – Automatically changes between long and short preamble mode transmission based on AP configurations. This is the default Preamble Mode.

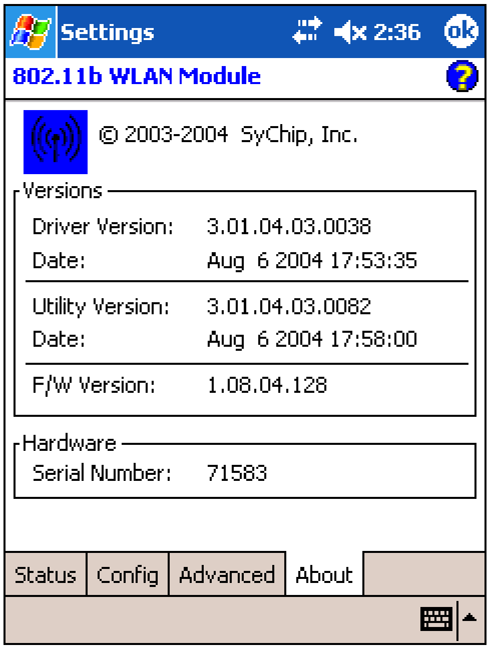
Defaults Resets all the settings to default values

- Always Enable for Power Save Mode,
- Automatic based on WEP setting for Authentication Algorithm, and
- Auto TX Preamble (for Preamble Mode).

Apply Applies changes. This button is active only when a change has been made on the tab.

About Tab

This window provides Version Number and time of build for Network Driver, Configuration Utility, and NIC Firmware.



© 2003-2004 SyChip, Inc.

Versions

Driver Version: 3.01.04.03.0038

Date: Aug 6 2004 17:53:35

Utility Version: 3.01.04.03.0082

Date: Aug 6 2004 17:58:00

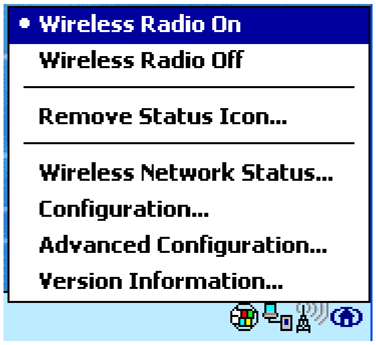
F/W Version: 1.08.04.128

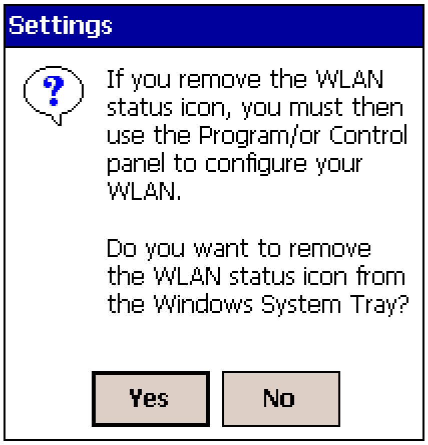
Hardware

Serial Number: 71583

The Status Icon

You access the 801.11b Settings by tapping and holding on the **Status** icon in the task tray at the bottom of the Today screen. The following menu pops up:



Menu Option	Selecting This Option…
Wireless Radio On	Turns on the radio. LED is on and the Link Icon displays with signal strength.
Wireless Radio Off	Turns off the radio. A pop-up window will ask for your confirmation. If confirmed, the LED will be off and the Status icon will change color from green to red on the top without signal strength displayed. The WLAN card/module will stop functioning.
Remove Status Icon	Removes the Status Icon from the bottom tray. A pop-up window asks you to confirm. Click **Yes** to confirm, or **No** to cancel. If confirmed, the Status icon does not display in the task tray, and you will need to go to **Start** > **Programs** > **802.11b Settings** in the future.  Settings If you remove the WLAN status icon, you must then use the Program/or Control panel to configure your WLAN. Do you want to remove the WLAN status icon from the Windows System Tray?
Wireless Network Status	Opens the Status tab of the configuration utility; see Status Tab on page 9-3.
Configuration	Opens the Config tab of the configuration utility; see Config Tab on page 9-5.
Advanced Configuration	Opens the Advanced tab of the configuration utility; see Advanced Tab on page 9-10.
Version Information	Opens the About tab of the configuration utility; see About Tab on page 9-11.

Note: The Status Icon changes to a crossed lock as a warning that you may have entered a wrong key (WEP Key mismatch) for the WEP-On AP or a station.

802.11b Wireless Security Supplement

AEGIS Client® offers the most comprehensive IEEE 802.1X supplicant for securing wired and wireless networks. The Client is a standards-based implementation of IEEE 802.1X and can be configured to work with almost any network equipment - wired or wireless - that supports the 802.1X authentication standard. The Client is interoperable with 802.1X-capable wireless access points and authentication servers including Microsoft's IAS and Cisco's ACS.

The Client solves the problem of key distribution in wireless LANs by using public key authentication and encryption between Wireless Access Points (WAP) and roaming stations to exchange dynamic Wired Equivalent Privacy (WEP) keys. In addition, network managers can control 802.1X user profiles from a centralized RADIUS server or, in the case of TTLS, from a RADIUS Diameter or other AAA servers. The Client supports both wireless (802.11a/b/g) and Ethernet interfaces.

System Requirements

You need the following equipment and software to run AEGIS Client software:

- A computer with a network interface card and/or wireless network interface card installed that support the NDIS 5.1 standard for 802.11 WLAN object identifiers (OID). The AEGIS Client software installation routine expects to find your computer’s wireless card properly installed, even if it isn’t connected to a network. If the card isn’t in the computer, the installation program can’t make the proper program and protocol associations. **Be sure your wireless card is installed!**
- The appropriate version of the AEGIS Client software package for your operating system. Contact HHP for the correct version for your company.

Platforms Supported

There are several versions of AEGIS Client software for computers using a wide variety of operating systems. Specific capabilities of a particular version of AEGIS Client may vary according to the operating system. This is due to varying levels of support for different EAP types by manufacturers. Drivers for some types of network hardware and operating system combinations don’t support as many EAP types as others combinations.

The following platforms are supported:

- Windows Mobile Software 2003 [OS version "Pocket PC Version 4.20.1081 (Build 13100)"]
- Pocket PC 2002 [OS version "Pocket PC Version 3.0.11171 (Build 11178)"]
- CE.NET 4.1 [OS version "CE .NET Version 4.10 (Build 908)"]
- CE.NET 4.2 [OS version "CE .NET Version 4.20 (Build 1088)"]

Note: Verify the operating system version by tapping **Start** > **Settings** > **System** tab > **About**.

802.1X Supplicant Protocol Support

Support for the Extensible Authentication Protocol (EAP) - RFC 2284

Supported authentication methods are as follows:

- CHAP/MD5 - RFC 1994
- EAP TLS Authentication Protocol - RFC 2716
- EAP Tunneled TLS (TTLS) - Internet Draft February 2002
- Cisco LEAP and PEAP
- Microsoft PEAP

Tested against the following servers:

- Funk Odyssey 3.2 using TLS, LEAP and TTLS
- AEGIS Client 1.1.4 using MD5, TLS, TTLS, LEAP and PEAP
- Cisco ACS 3.2 using MD5, TLS, LEAP and PEAP

⚠ If you are using one of these authentication methodologies, you need to configure your 802.11b connection here, NOT through HHP WLAN Settings. However, if you want to set the AP Search Threshold above the default setting of Low Density, you do need to change that setting in HHP WLAN Settings; for details, see Network Profile Tab on page 9-7.

Required Network Configuration Information Worksheets

Because AEGIS Client enables your terminal to access a network that is protected by the IEEE 802.1X protocol, you must configure EAP data communication to match your network server parameters. If the EAP configuration doesn't match your network configuration, you can't access the network.

Installing and configuring the Client usually takes less than 15 minutes, provided you have the required equipment, software, and configuration information. You need clear information from the network administrator about how the network's authentication works.

The worksheets on the following pages provide space to record the required Client configuration information to set up the Client to match specific Extensible Authentication Protocols (EAP). The forms are designed so that hard copies can be filled out, copied, and distributed.

The client software supports the following EAP authentication methods:

- MD5
- LEAP
- TLS/SmartCard
- TTLS
- PEAP

There is a worksheet for each method. Complete the worksheet for the method you choose.

MD5 Worksheet

To configure AEGIS Client to use MD5 authentication, you need to know:

1. Will you use your Windows user name and password for network authentication? (Applies only to Windows clients.)
2. If not, what is your unique user name/password combination?

If a second set of credentials is required, you need to know the exact user name and password. These are typically case-sensitive.

User name: _______________________________________

Password: ____

LEAP Worksheet

To configure AEGIS Client to use LEAP authentication, you need to know:

1. Will you use your Windows user name and password for network authentication? (Applies only to Windows clients.)
2. If not, what is your unique user name/password combination?

If a second set of credentials is required, you need to know the exact user name and password. These are typically case-sensitive.

User name: _______________________________________

Password: ____

TLS/SmartCard Worksheet

To configure AEGIS Client to use TLS/SmartCard authentication, you need to know:

1. Is a client certificate required?

____ No.

____ Yes. This file needs to be installed on your machine by your network administrator.

2. Should the AEGIS Client validate the server certificate chain?

____ No. Skip Questions 3-4.

____ Yes.

3. Will the server accept any trusted Certificate Authority (CA), or is a particular CA required?

____ Any trusted CA is acceptable.

____ A particular CA is required:________________________

4. Are intermediate certificates allowed?

____ No.

____ Yes.

5. What is the name of the server? _____________________________
This usually includes the server's domain, for example: server.big_school.edu.

TTLS Worksheet

To configure with TTLS authentication, you need to know:

1. Use Windows user name and password for authentication? (Applies only to Windows clients.)
2. If not, what is your unique user name? If a second set of credentials is required, you need to know the exact user name. This is usually case-sensitive.

User name:_______________________________________

3. Is a client certificate required?

____ No.

____ Yes. This file needs to be installed on your machine by your network administrator.

4. What is the user name (identity) and password for the tunnel authentication?

User name:_______________________________________

Password:____

5. What is the tunnel authentication protocol?

____ CHAP (Challenge Handshake Authentication Protocol)

____ MS-CHAP (Microsoft CHAP Extensions)

____ MS-CHAP v2 (Microsoft CHAP Extensions v. 2)

____ PAP

____ EAP-MD5

6. Is a server certificate is required?

____ No.

____ Yes.

7. Should the Aegis Client validate the server certificate chain?

____ No. Skip Questions 8-9.

____ Yes.

8. Will the server accept any trusted Certificate Authority (CA), or is a particular CA required?

____ Any trusted CA is acceptable.

____ A particular CA is required: _______________________

9. Are intermediate certificates allowed?

____ No.

____ Yes.

10. What is the name of the server?

This usually includes the server's domain, for example: server.big_school.edu. ______________________________

PEAP Worksheet

To configure AEGIS Client with PEAP Authentication, you need to know:

1. Use Windows user name and password for authentication? (Applies only to Windows clients.)
2. If not, what is your unique user name? If a second set of credentials is required, you need to know the exact user name. This is usually case-sensitive.

User name:____

3. Is a client certificate required?

____ No.

____ Yes. If it is, this file needs to be installed on your machine by your network administrator.

4. What is the user name (identity) and password for the tunnel authentication?

User name:____

Password:____

5. What is the tunnel authentication protocol?

____ MS-CHAP v2 (Microsoft CHAP Extensions v. 2)

____ EAP TLS/SmartCard

____ Generic Token Card

6. Is a server certificate is required?

____ No.

____ Yes.

7. Should the Aegis Client validate the server certificate chain?

____ No. Skip Questions 8-9.

____ Yes.

8. Will the server accept any trusted Certificate Authority (CA), or is a particular CA required?

____ Any trusted CA is acceptable.

____ A particular CA is required: ________________________

9. Are intermediate certificates allowed?

____ No.

____ Yes.

10. What is the name of the server?

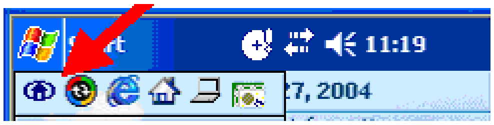
This usually includes the server's domain, for example: server.big_school.edu. ______________________________

Opening the Client

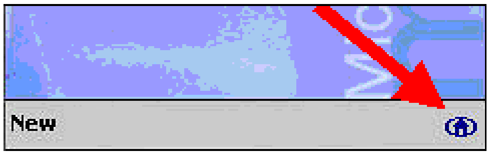
To access the client the first time, tap **Start** > **Programs** > **Meetinghouse AEGIS Client** Meetingho... AEGIS Client.

After the Client has been activated, you can:

1. Tap **Start**. The icon appears in the quick start tray on the Start menu. Tap the icon to open the Client.



2. Tap the icon in the lower left corner of the command bar.



Icon Indicators

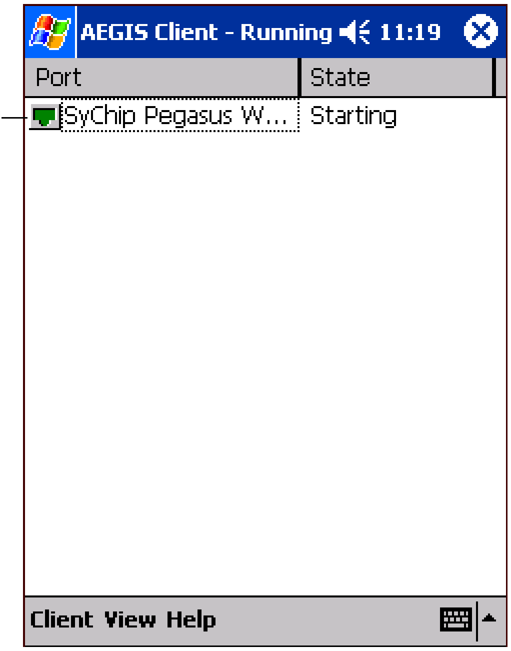
The color of the icon indicates the status of the controlled ports.

Icon	Color	This color icon indicates that ...
🟢	Green	Authentication succeeded.
🟡	Yellow	Authentication is in process.
🔴	Red	Authentication failed.
If there is no yellow, red or green in the icon then either the ports are not being controlled by 802.1X, or there is no authentication activity on the controlled ports. The absence of yellow, red or green may also indicate that the network access server is not an 802.1X aware device.		
⚪	Gray	The port is not in use or is disabled. Either the Client isn't running, or the port is not bound to the 802.1X protocol.
🟠	Orange	The port is associated, but there is no response to 802.11b packets. If using WEP without 802.1x authentication, this will be the final state when the connection is complete. If using 802.1x authentication, it is either a transient condition or can indicate that attempts to authenticate have timed out as there was no response to 802.1X packets.
🔵	Blue	There is no 802.11b activity. The port may not be connected to an 802.1X-aware entity.

Note: Different parts of the icon can have different colors if more than one interface on the system is running 802.1X. For example, if your terminal has more than one active network interface card (NIC) then different parts of the icon will have different colors corresponding to the state of each NIC.

The Main Screen

On the terminal, open the Client. The main screen opens displaying a list of ports on the system’s network interface cards, You manage ports on this screen.



Port	State
SyChip Pegasus W...	Starting

Port Status icon

Port Status Icon

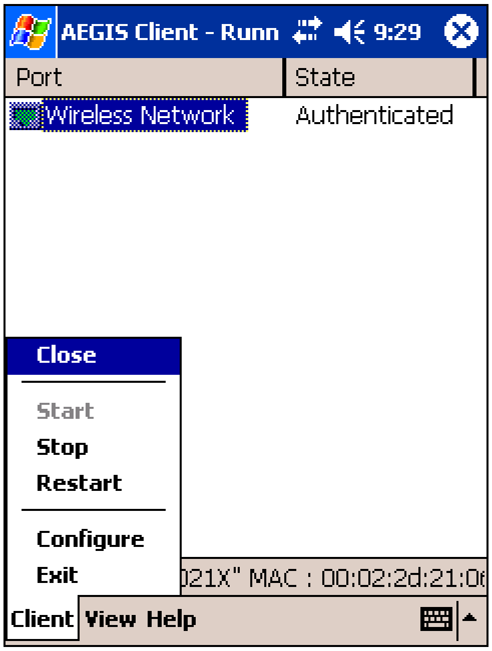
The main screen contains a port status icon to the left of each port listed. The color of this icon indicates the status of the port.

The color of the icon changes as the port starts authentication, negotiates with the access point and/or authentication server, and then joins the network. As the network interface starts or stops, the color of the port icon and the status field in the Interface List updates to reflect the current state of the interface.

For details about what each color means, see Icon Indicators on page 9-18.

Client Menu

To open the client menu, tap **Client** in the command bar along the bottom of the window.

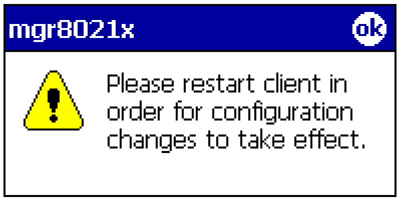


Menu Item | **Tapping this item…**

Close — Closes the Client's interface, while leaving the client running.

Start/Stop — Starts or stops 802.1X authentication. After you finish the initial configuration, tap the network interface and tap **Start.** If the port is already active, tap **Stop** first, then **Start** to force the program to read the new configuration file.

Restart — Same as a Stop followed by Start. Tap this when you receive a notice such as the following:



mgr8021x

Please restart client in order for configuration changes to take effect.

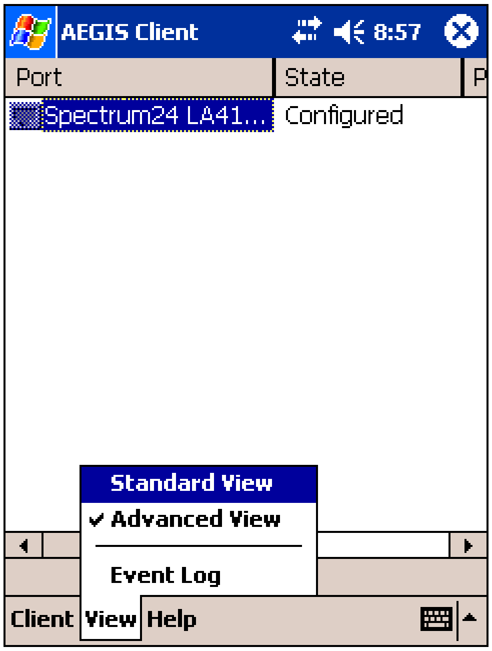
Configure — Opens the Configuration screen displaying the User tab.

Install Protocol — Selecting this option binds the 802.1X protocol to the WLAN adapter currently installed on the device. The WLAN adapter then appears in the port list. For more information about network adapters, see Network Cards on page 7-35.

Exit — Terminates the client, which stops the 802.1X protocol.

View Menu

To access the View menu, tap **View**.

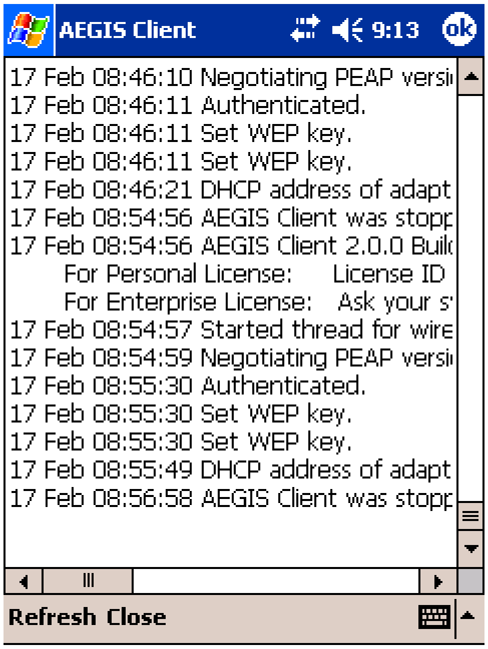


The Standard and Advanced Views control the number of columns displayed in the main menu.

Menu Item	**Tapping this item…**
Standard View	Displays the **Port** (adapter name) and **State** columns. This is the default view.
Advanced View	**Displays the Port** (adapter name), **State**, **Primary Wireless Network**, **Wireless Network**, and **MAC Address of AP** columns. Scroll right to see all columns.

Event Log

The Event Log is a text file that contains status information from the logging function. Each entry is listed sequentially with a time stamp and a text message.



```
17 Feb 08:46:10 Negotiating PEAP versi
17 Feb 08:46:11 Authenticated.
17 Feb 08:46:11 Set WEP key.
17 Feb 08:46:11 Set WEP key.
17 Feb 08:46:21 DHCP address of adapt
17 Feb 08:54:56 AEGIS Client was stopp
17 Feb 08:54:56 AEGIS Client 2.0.0 Buil
        For Personal License:     License ID
        For Enterprise License:   Ask your s
17 Feb 08:54:57 Started thread for wire
17 Feb 08:54:59 Negotiating PEAP versi
17 Feb 08:55:30 Authenticated.
17 Feb 08:55:30 Set WEP key.
17 Feb 08:55:30 Set WEP key.
17 Feb 08:55:49 DHCP address of adapt
17 Feb 08:56:58 AEGIS Client was stopp
```

Tap **Refresh** to retrieve the most current information and display it in the log immediately.

Tap **Close** to return to the main screen.

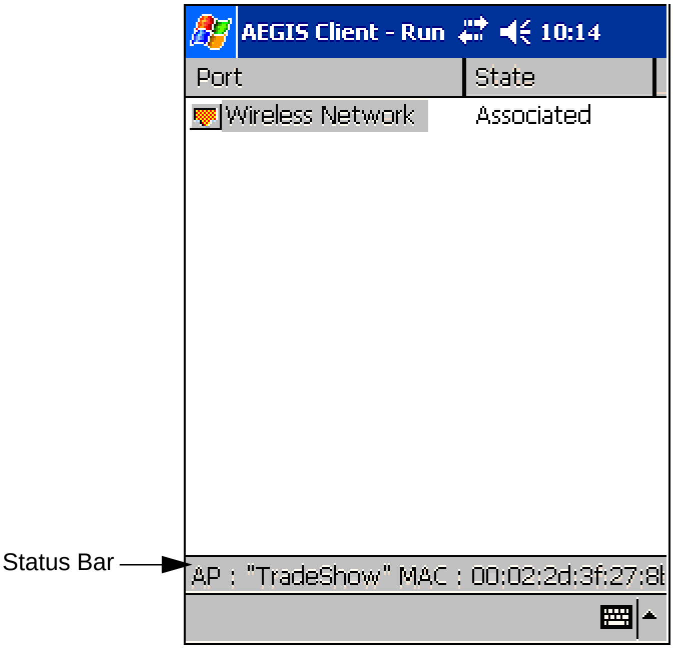
For more information about logging, [INSERT CROSS-X]

Help Menu

Tapping Help opens the help menu. Select **Online Help** to access online help. Select **About** to review software version information.

Status Bar

The status bar is displayed at the bottom of the main screen and indicates the connection status between the network card and the access point.

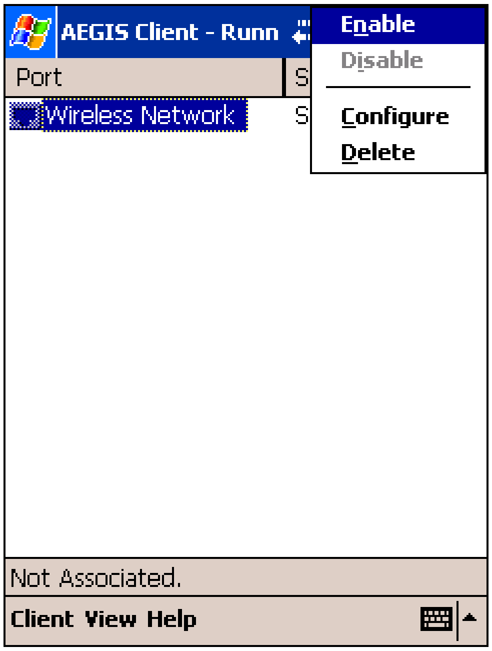


The status bar displays one of the following depending on the status of connectivity:

- “Not Associated”
- “AP : [Name of the SSID] MAC : [MAC address].”

Port Menu

On the main screen, tapping on a port opens a popup menu that allows the port to be enabled or disabled, configured, or deleted.



Not Associated.

The port menu enables you to use 802.1X authentication, change the port configuration, or remove it from the port list. If there are no entries in the Port list, follow the advice in the troubleshooting section to resolve the problem.

The Port menu options are:

Enable and Disable These commands enable or disable 802.1X authentication on the port. The port should be enabled before the protocol is started. Enabling a port is not the same as starting it (see Client Menu on page 9-20); however, both actions are required for the Client to work.

Configure Opens the port configuration screen. For details [CROSS X TO PORT SETTINGS SECTION]

Delete Removes an adapter from the port list. An unused port may be deleted from the port list. The radio card must not be in the device or the radio must be turned off.
Ports appear in the list only when the 802.1X protocol binds to the adapter. The protocol binds to the adapter when the adapter is in the device and the Client software is installed, or Install Protocol is selected from the Client menu (see Client Menu on page 9-20).

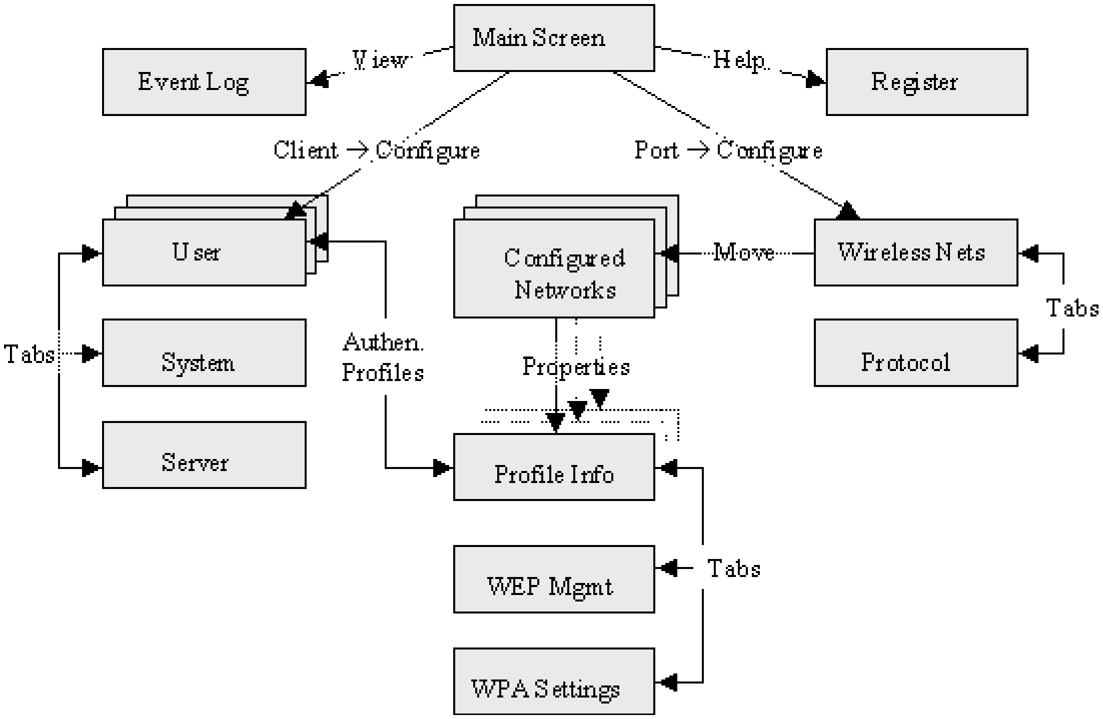
Configuring the Client

The Client is configured in two separate areas:

1. **Client Configuration** area - enables you to configure user settings and is accessed from the Client menu in the command bar.
2. **Port Settings** area - enables you to configure Network Properties settings for individual wireless networks and is accessed from the Port menu.

Configuration Screens

Both Client Configuration and Port Settings areas lead you through a series of setup screens. The following diagram displays the different screens and how they are related:



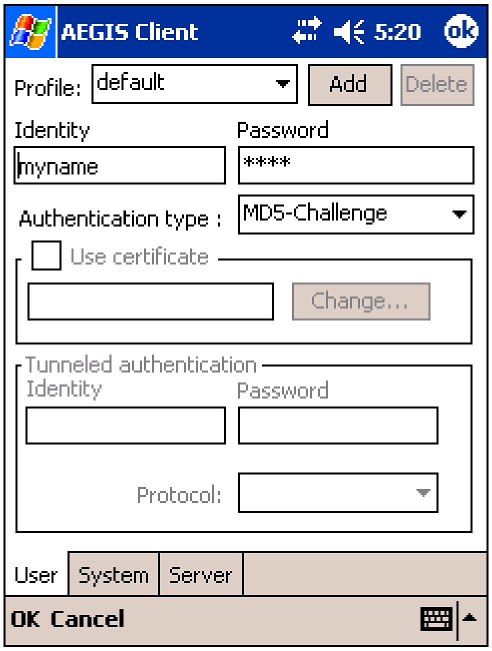
Client Configuration Area

Each user account needs to define the protocol and the credentials used to authenticate a user. Because Windows Mobile devices are usually small devices with a single NIC and, usually, a single user, the initial configuration is usually the only time the software needs to be set up. The Client will need to be reconfigured if the device is used on multiple networks, or if different users share the computer.

Note: Fields are be grayed out if not relevant to the selected protocol.

Accessing the Client Configuration Area

On the main screen, tap **Client** > **Configure** (see Client Menu on page 9-20). The Client Configuration screen opens displaying the User tab.



Profile: default

Identity: myname

Password: ****

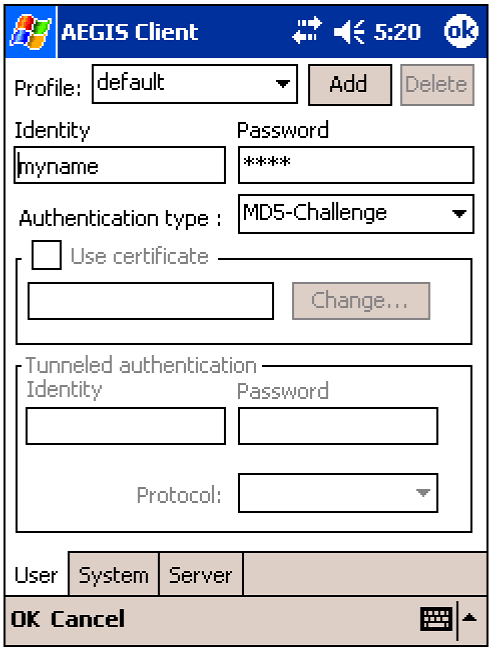
Authentication type : MD5-Challenge

□ Use certificate

On this tab,	**You…**
User Settings Tab	Configure authentication credentials and profiles.
System Settings Tab	Set the level of detail that the Client will provide in the system log and zero-config options.
Server Identity Tab	Control how the Client authenticates the server that handles the 802.1X protocol on the network side. This applies only to the TLS, TTLS, and PEAP authentication methods and is used to tell the Client what server credentials to accept from the authentication server to verify the server.

User Tab

The User settings tab defines the protocol and the credentials used to authenticate a user.



Profile: default

Identity: myname

Password: ****

Authentication type : MD5-Challenge

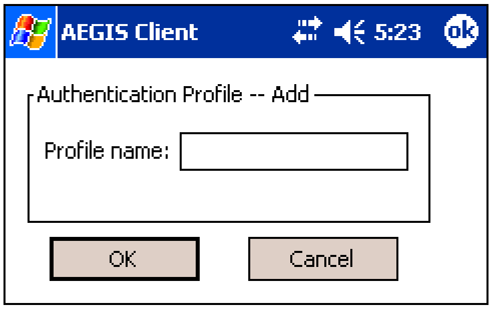
□ Use certificate

Field **Description**

Profile

Multiple user credential profiles can be created for use when the user roams from one network to another. The drop-down list contains existing authentication credential profiles. Select a profile from the list to edit it in the fields that follow.

Tapping **Add** permits new profiles to be added to the list. A screen appears where you can enter a name for the new profile.



Authentication Profile -- Add

Profile name:

Enter a **Profile name** and tap **OK**. The name entered appears in the Profile drop-down list.

Tapping **Delete** deletes authentication profiles. To be deleted, a profile **cannot** be assigned to a configured network.

Field | **Description**

Identity

This is the 802.1X identity supplied to the authenticator. The identity value can be up to 63 ASCII characters and is case-sensitive.

For tunneled authentication protocols such as TTLS and PEAP, this identity (called the Phase 1 identity) is sent outside the protection of the encrypted tunnel. Therefore, it is recommended that this field not contain a true identity, but instead the identity “anonymous” and any desired realm (e.g. anonymous@myrealm.com). For TTLS and PEAP, true user credentials (Phase 2 identity) are entered in the Tunneled authentication section.

Note: When used with PEAP and the .NET Enterprise Server Version 5.2, this field must contain the identity used in both Phase I and Phase II. The Phase II identity field is ignored.

Password

This is the password used for MD5-Challenge or LEAP authentication. It may contain up to 63 ASCII characters and is case-sensitive. Asterisks appear instead of characters for enhanced security.

Authentication type

This is the authentication method to be used - MD5-Challenge, LEAP, PEAP, TLS, or TTLS.

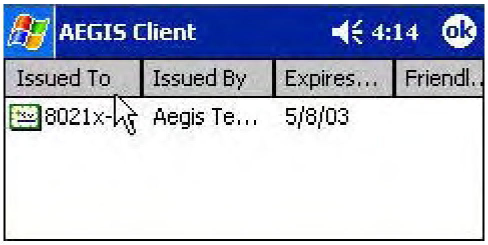
Your network administrator should let you know the protocols supported by the RADIUS server. The RADIUS server sits on the network and acts as a central credential repository for Access Servers that receive the radio signals and ultimately block or allow users to attach to the network.

Use certificate

This is the certificate to be used during authentication. A certificate is required for TLS, optional for TTLS and PEAP, and unused by MD5 and LEAP. Therefore, this option becomes active only when TLS, TTLS, or PEAP is selected as the Authentication type.

If **Use certificate** is enabled, the client certificate displayed in the field is the one that is passed to the server for verification.

To select a client certificate, tap **Change** and select the certificate from the list that appears.



Issued To	Issued By	Expires...	Friendl..
8021x-	Aegis Te...	5/8/03	

To appear in this list, certificates must be installed in the system, for a description of this process see Installing Certificates with CertAdd on page 9-41.

The **Issued to** field should match the **Identity** field and the user ID on the authentication server (i.e., RADIUS server) used by the authenticator.

Your certificate must be valid with respect to the authentication server. This generally means that the authentication server must accept the issuer of your certificate as a Certificate Authority.

Note: When obtaining a client certificate, do not enable strong private key protection. If you enable strong private key protection for a certificate, you will need to enter an access password for the certificate each time this certificate is used.

Tunneled authentication area

Tunneled authentication parameters are used by only by TLS, TTLS and PEAP protocols, in Phase 2 of authentication, and after the secure tunnel has been established. The fields in this section are active only if the TLS, TTLS, or PEAP is selected as the Authentication type.

Identity

The user identity used in Phase 2 authentication. The identity specified may contain up to 63 ASCII characters, is case-sensitive and takes the form of a Network Access Identifier, consisting of <name of the user>@<user’s home realm>. The user’s home realm is optional and indicates the domain to which the tunneled transaction is to be routed.

Note: Because Microsoft .NET Enterprise Server Version 5.2 does not use this parameter for PEAP, This field will have no effect for PEAP at this time. Phase 1 identity is used instead.

Field — **Description**

Password

The password used for the tunneled authentication protocol specified. It may contain up to 63 ASCII characters and is case-sensitive. Asterisks appear instead of characters for enhanced security.

Protocol

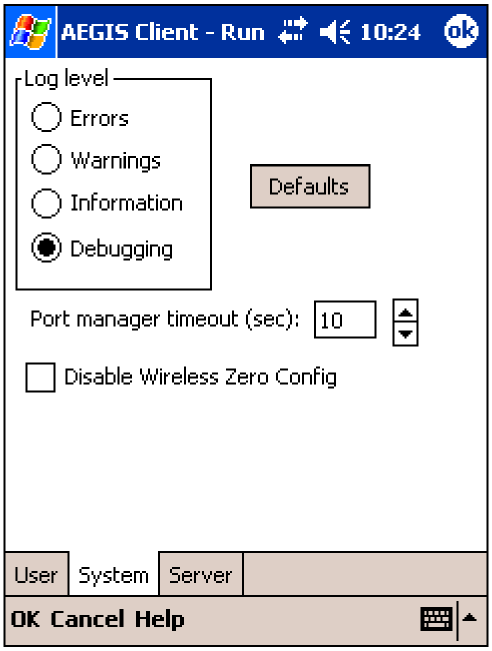
This parameter specifies the authentication protocol operating within the secure tunnel.

The following protocols are currently supported for TTLS: EAP-MD5, CHAP, PAP, MS-CHAP and MS-CHAP-V2.

The following protocols are currently supported for PEAP: EAP-MS-CHAP-V2, TLS/Smartcard, and Generic Token Card (EAP-GTC).

System Tab

The System Settings tab controls logging and the port manger timeout period.



Log level

○ Errors

○ Warnings

○ Information

● Debugging

Port manager timeout (sec): 10

□ Disable Wireless Zero Config

Field — **Description**

Log Level

These settings control the detail of the log messages generated by the Client. Each level is cumulative. By default, all errors, warnings, and information events are logged. Each entry records a severity code (of one [debug message] to four [error] asterisks), a time stamp, and a message.

Errors - only the most severe conditions are logged.

Warnings - less severe conditions are logged.

Information - all errors, warnings, and information events are logged. This is the default setting.

Debugging - creates a log message each time the Client detects or reacts to an event. Be advised that log entries fill memory quickly if the Debugging level is chosen. Do not use the Debugging option for a significant length of time because most internal operations generate messages.

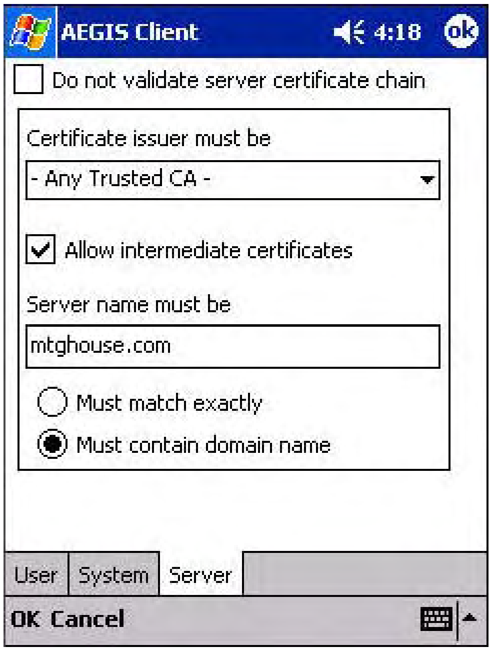
Defaults

Tap this button to return log settings to the default settings.

Field	Description
Disable Wireless Zero Config	Use this option only as directed by technical support. Selecting this option disables other wireless utilities whether the Client is running or not. If not selected, other wireless utilities cannot apply their settings to the wireless card while the Client is running (although their status displays are usually unaffected). You will need to perform a soft reset whenever this setting is changed.
Port Manager Timeout	The interval at which the client polls the ports. This is used under different circumstances, for instance after physical changes such as card removal or insertion have been detected. This value should not be changed from the 10-second default unless so advised by technical support.

Server Tab

The Server identity tab defines the credentials the client uses to authenticate the server during TLS/TTLS/PEAP authentication message exchange. The Client uses this information to verify that the Client is communicating with a trusted server.



□ Do not validate server certificate chain

Certificate issuer must be
- Any Trusted CA -

☑ Allow intermediate certificates

Server name must be
mtghouse.com

○ Must match exactly
● Must contain domain name

Field	Description
Do not validate server certificate chain	If this option is selected, the server certificate received during the TLS/TTLS/PEAP message exchange is not validated.
Certificate issuer must be	This is the certificate authority used during TLS/TTLS/PEAP message exchange. **Any Trusted CA** is the default selection and means that any certificate authority can be used during authentication. Both trusted intermediate certificate authorities and root authorities whose certificates exist in the system store are available for selection in the drop-down list.
Allow intermediate certificates	This option is selected by default. It enables a number of unspecified certificates to be in the server certificate chain between the server certificate and the certificate authority indicated in the **Certificate issuer must be** field. This allows the server certificate received during negotiation to be issued directly by the certificate authority or by one of its intermediate certificate authorities. If disabled, then the selected Certificate issuer must have directly issued the server certificate.

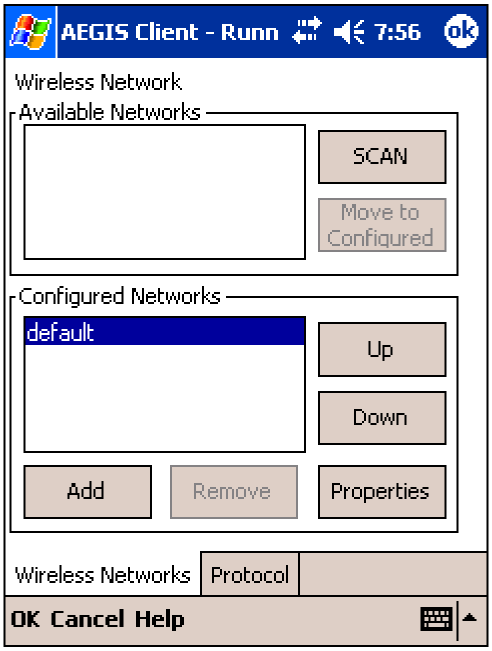
Field	Description
Server name must be	This is either the server name or the domain the server belongs to, depending on which option is selected below the text field. During authentication, this name will be compared to the server certificate’s **Subject: CN** field.
Must match exactly	When selected, the server name entered must match the server name found on the certificate exactly.
Must contain domain name	When selected, the server name field identifies a domain and the certificate must have a server name belonging to this domain or to one of its sub-domains (e.g., zeelans.com, where the server is blueberry.zeelans.com).

Port Settings Area

In the Port Settings area, you configure network parameters for each port listed on the main screen; see The Main Screen on page 9-19.

Accessing the Port Settings Area

1. On the main screen, tap and hold on a port. The Port popup menu appears; see Port Menu on page 9-24.
2. Tap **Configure**. The Port Settings Configuration screen opens displaying the Wireless Networks tab.



On this tab,	You…
Wireless Networks Tab	Set the parameters for Network Access Points and underlying protocol.
Protocol Tab	Configure common protocols that apply to any network the port connects to.

Wireless Networks Tab

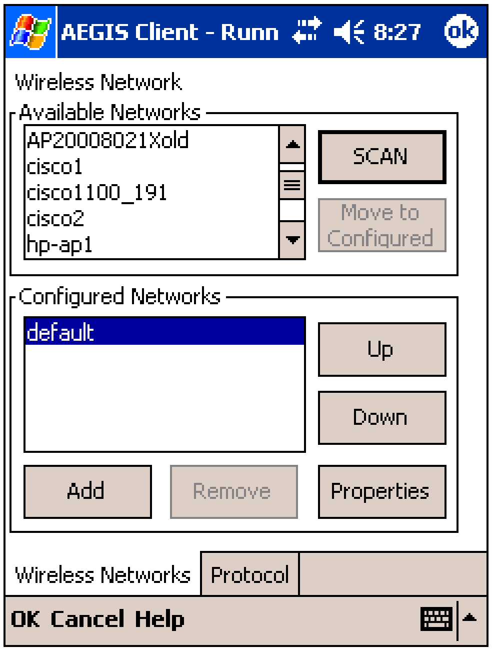
Field **Description**

Available Networks Section

This section displays the networks the terminal recognizes as available to connect to. When the Client is first installed, there are no entries in the Available Networks list.

Scan

Tap this button to see a list of networks broadcasting their availability.



AEGIS Client - Runn 8:27

Wireless Network

Available Networks

AP20008021Xold
cisco1
cisco1100_191
cisco2
hp-ap1

Configured Networks

default

Note: You can also attach to networks who are not broadcasting.

Move to Configured

This button activates only after **Scan** has been tapped and available networks have been retrieved.

In the list of networks retrieved, select the network you wish to connect to, and tap **Move to Configured**. This selects the network, which now appears in the Configured Networks section.

Configured Networks section

This section displays the networks your terminal is connected to. This section enables you to add or remove networks as well as review and edit the properties of existing configured networks.

Default

When the Client is first installed, there is a Configured Network named "default" in the list. This profile has **Associate with any network** selected in its Properties selection screen.

If you are going to be in a location with only one access point (or more than one access point that attaches to the same network), the default profile may be sufficient for you needs, without necessitating the selection of a specific network or networks.

If **default** is last in the list, it can act as a wildcard should you be out of the range of your primary networks (which are listed first). Do not place **default** at the top or middle of the list because, if it is, connection to the other list entries will never be attempted.

Up

Tapping this button moves a selected network up one place in the list.

Down

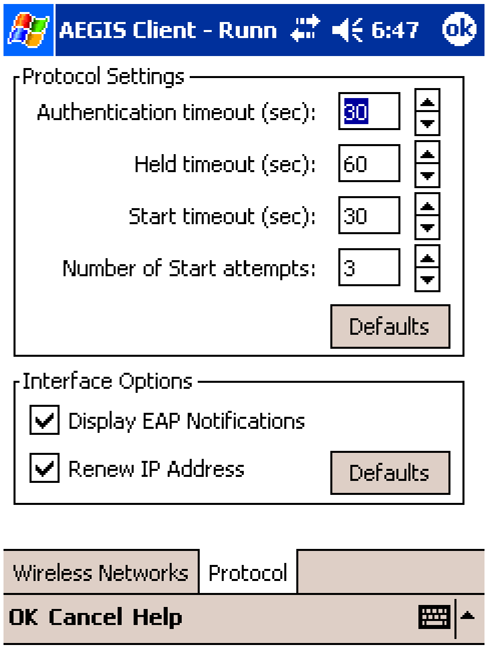
Tapping this button moves a selected network down one place in the list.

Note: The order of the networks in this list is the exact order that connections will be attempted. The network listed first will be attempted first and so on. Place your primary networks first.

Field	Description
Add	Tap this button to manually add a network to the Configured Networks list if • the access point does not broadcast its SSID or • you are pre-configuring the client for an access point that is not currently in range. For more information, see Adding a Wireless Network Configuration on page 9-36.
Remove	Tap this button to remove a selected network in the list.
Properties	Tap this button to review the properties of a network selected in the list. This button opens the same network configuration screen as the **Add** button does; use it to edit network configuration properties.

Protocol Tab

The Protocol tab enables you to configure parameters that will apply to all the networks the selected port connects to.



AEGIS Client - Runn 6:47

Protocol Settings

Authentication timeout (sec): 30

Held timeout (sec): 60

Start timeout (sec): 30

Number of Start attempts: 3

Interface Options

☑ Display EAP Notifications

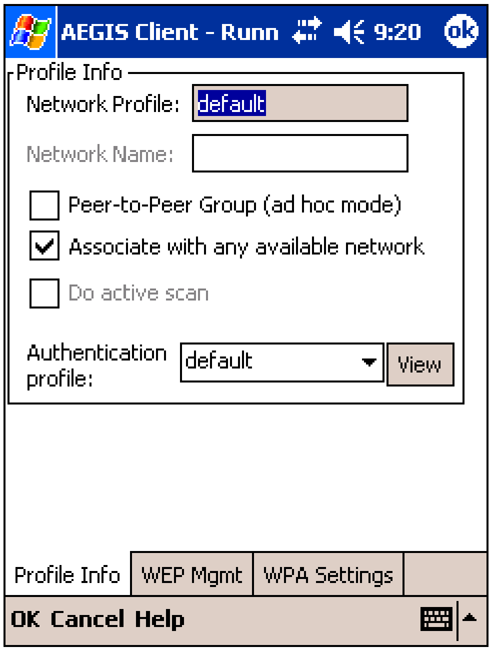
☑ Renew IP Address

Field	Description
Protocol Settings	These are the timer intervals and retry settings defined in the 802.1X standard. They determine how long the supplicant state machine will wait in a given state. These parameters shouldn't be modified without an understanding of the supplicant state machine. For more information about the supplicant state machine, obtain its 802.1X protocol specification. The parameters are: • **Authentication Timeout -** The period of time the Client remains in the authenticating or acquired state without receiving a response from the access point or switch. • **Held Timeout** - The period of time the Client remains in the held state after failing authentication. • **Start Timeout** - The period of time the Client remains in the connecting state before restarting when there is no response. • **Number of Start Attempts** - The number of times the Client restarts before giving up. At that point, the Client then defaults to the authenticated state, but there will be no network connectivity because the protocol exchange was never completed.

Field	Description
Display EAP notifications	This option specifies that the EAPOL notification message will be displayed to the user. An authenticator may use such notification to inform you, for example, about a near password expiration. However, some authenticators send chatty and annoying notifications that may, for the convenience of the user, be suppressed. Note that all notifications are written to the event log even if they are not displayed.
Renew IP address	Select this option to initiate a DHCP request to obtain a dynamic IP address after a successful authentication, but only if the client detects that the connected network (the SSID) has changed. The result is that renewal should not occur upon re-authentication, but does occur at boot or when connecting to a different network. If you have a slow authenticator, you may wish to enable this option when configuring the service because a slow authenticator may prevent you from getting a DHCP-assigned IP address upon boot-up. This option is ignored if the given adapter has a static IP address.

Adding a Wireless Network Configuration

To add a wireless network configuration, on the main screen, tap and hold on the port, tap **Configure** on the Port popup menu, then tap **Add** in the Network Configurations section of the Wireless Networks tab. The Network Profile screen opens displaying the Profile Info tab.



Profile Info

Network Profile: default

Network Name:

□ Peer-to-Peer Group (ad hoc mode)

☑ Associate with any available network

□ Do active scan

Authentication profile: default

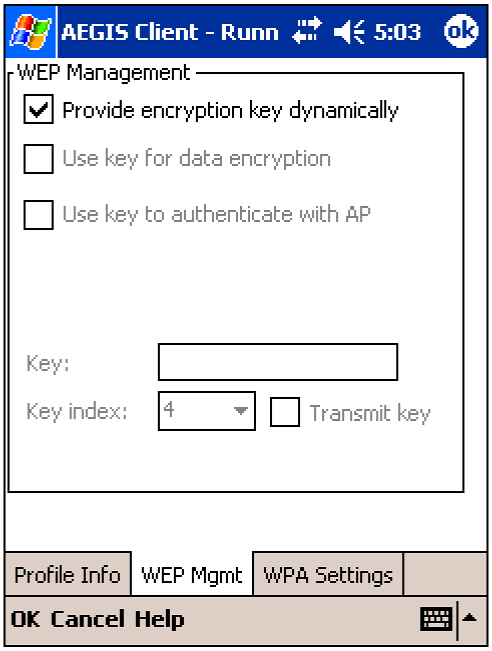
On this tab,	You…
Profile Info	Enter basic profile information for your wireless connection.
WEP Mgmt	Enter the WEP settings for your wireless connection - see page 9-37.
WPA Settings	Enter the WPA settings for your wireless connection - see page 9-39.

Profile Info Tab

Field	Description
Network Profile	Enter the name of this record. This is the name that appears in the Configured Networks list and, by default, is the same as the broadcast SSID. Note that there is nothing special about the name "default". You could configure any other record similarly and it would behave the same way.
Network Name	This is the SSID of the access point. If the access point broadcasts its SSID, then this value may be derived from the Available Networks list. If the SSID does not broadcast, then you must manually enter the value here.
Peer-to-Peer Group (ad hoc mode):	Select this option to have two or more client workstations communicate with each other without the benefit of an access point. You should also select **Do Active Scan** and, in the WEP Management page, enable **Use key for data encryption** while entering a common key for both sides. WPA is not supported in this mode.
Do active scan	Select this option whenever the access point (or client, for ad hoc mode) is not broadcasting its SSID.
Authentication Profile	Select the Client Configuration (user) profile associated with this network. The drop-down list contains client profile names created in the User tab of the Client Configuration Area; see User Tab on page 9-27. To open the selected profile, select it in the drop-down list and tap **View**. The User tab opens displaying the profile details. If you tap **OK** (to save changes) or **Cancel**, you are returned to the Profile Info tab.

WEP Mgmt Tab

The WEP Mgmt tab enables you to set WEP parameters for each port.



WEP Management

☑ Provide encryption key dynamically

□ Use key for data encryption

□ Use key to authenticate with AP

Key:

Key index: 4 □ Transmit key

Note: The settings on this tab window are interrelated. This means that selecting one may disable access to others.

Field — **Description**

Provide encryption key dynamically

This option is selected by default. If this option is selected, the other WEP settings on this page are disabled. To enter a custom WEP, de-select this option. The other fields become active.

Use key for data encryption

Select this option to manually enter a WEP key to encrypt your data to the access point. You enter that key in the Key field below.

Use key to authenticate with AP

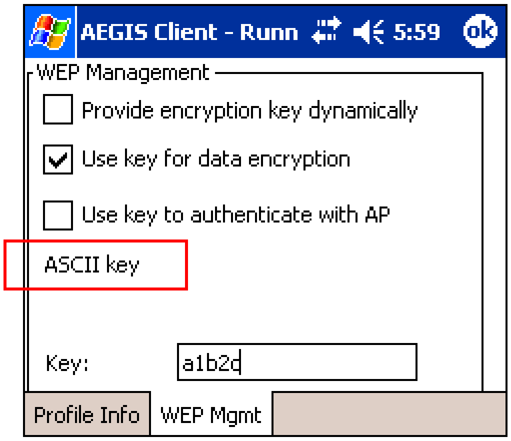
Select this option if your network does not support 802.1x authentication and you need to connect to the access point without username and password authentication. The key entered below is used to authenticate instead.

Key

In this field, enter the WEP key:

- ASCII - 5 or 13 characters
- Hexadecimal - 10 or 26 characters.

When the key entered is in the correct format, the screen changes to display the type - ASCII or Hexadecimal. For example,



AEGIS Client - Runn 5:59

WEP Management

□ Provide encryption key dynamically

☑ Use key for data encryption

□ Use key to authenticate with AP

ASCII key

Key: a1b2c

Key Index/Transmit Key

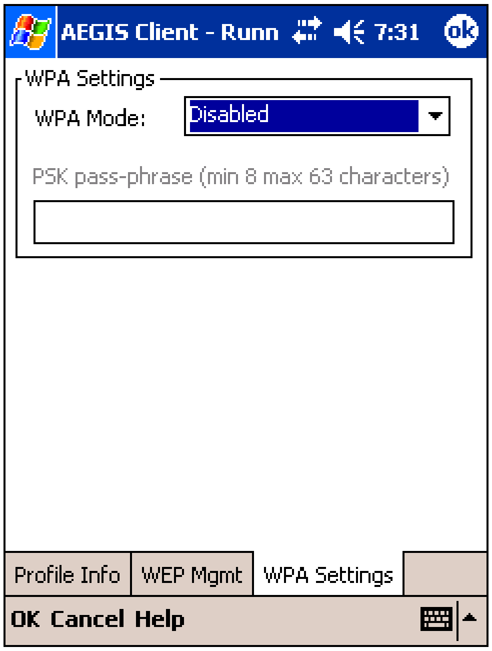
The Key Index drop-down list contains the available keys. You may enter up to four keys for reception; the Client will try all four to find one that works with the access point.

From the drop-down list, select the key to be used for transmission as well. If the key selected is the transmit key, the **Transmit key** box is checked.

To change the transmit key, select another key and check the **Transmit key** box. The check box of the original transmit key will be automatically de-selected.

WPA Settings Tab

The WPA Settings tab enables you to configure WPA settings.



WPA Mode: Disabled

PSK pass-phrase (min 8 max 63 characters)

Field	Description
WPA Mode	This drop-down list contains the following options: • **Disabled** - Do not enable WPA mode. This is the default selection. • **WPA 802.1x** - Enable WPA and obtain key information through the 802.1x protocol. • **WPA PSK** - Enable WPA with Pre-Shared Key (PSK) information entered in the field below. This mode is used if the 802.1x protocol is not being used for authentication.
PSK pass-phrase	This field activates if you select WPA PSK in the WPA Mode drop-down list. Enter between 8 and 63 characters for your pass phrase. Asterisks appear as you type for increased security.

Logging

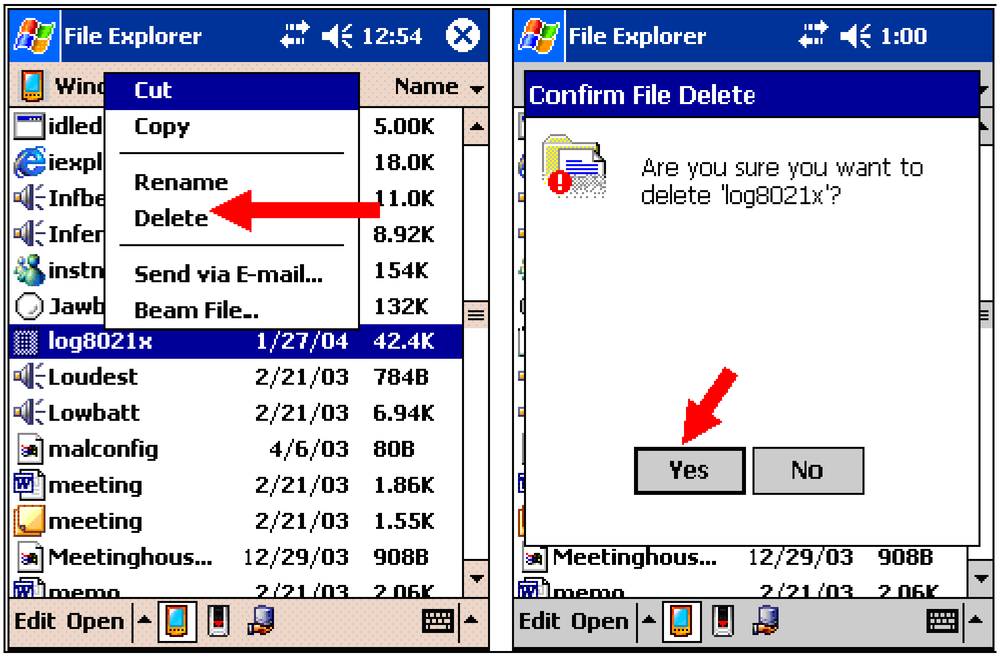
The event log is an ASCII text file named “LOG8021X.TXT” located in the directory defined by the WINDIR environment variable (usually the Windows directory). The information the log records is determined by the log settings on the System tab of the Client Configuration Area; see System Tab on page 9-29.

The format of the entries is

```
Time Stamp          Message Text
```

The **Refresh** button at the bottom of the screen is used to update the log file while you are reading it. If the file gets too large, old entries are automatically deleted.

If you wish to start with a blank file, exit from the Client (so the icon no longer appears at the lower right of the screen) and delete the log file (log8021x) in File Explorer; see Finding and Organizing Information on page 4-16.



idled		5.00K
iexpl		18.0K
Infbe		11.0K
Infer		8.92K
instn		154K
Jawb		132K
log8021x	1/27/04	42.4K
Loudest	2/21/03	784B
Lowbatt	2/21/03	6.94K
malconfig	4/6/03	80B
meeting	2/21/03	1.86K
meeting	2/21/03	1.55K
Meetinghous...	12/29/03	908B
memo	2/21/03	2.06K

Confirm File Delete

Are you sure you want to delete 'log8021x'?

When you restart the Client, a new log file is created.

Installing Certificates with CertAdd

Certificate Requirements

During configuration, you may have specified one or two certificates to use during the authentication process. The specified identity should match the **Issued to** field in the certificate and should be registered on the authentication server (i.e., RADIUS server) that is used by the authenticator. In addition, your certificate must be valid on the authentication server. This requirement depends on the authentication server and generally means that the authentication server must know the issuer of your certificate as a trusted Certificate Authority.

If the selected certificate does require a password or pass phrase to decode the private key, enter this value in the "Certificate Pass Phrase" field. This value will be encrypted when the configuration is saved. However, on some systems, there may not be a certificate. If that is the case, you can use the section below as a primer on OS X certificate management.

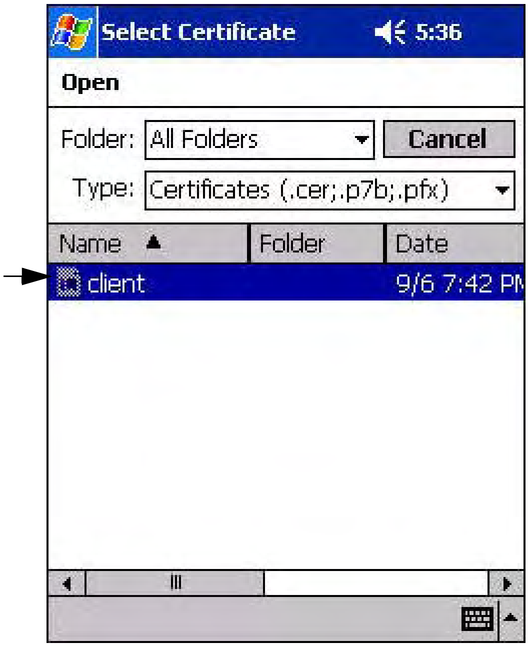
About CertAdd

CertAdd is a stand-alone utility included with the Client that allows certificates to be selected and installed on a Windows Mobile device.

Installing Certificates with CertAdd

Client or Certificate Authority (CA) certificates can be imported from *.cer (same as *.der), *.p7b, or *.pfx files.

1. Download the certificate file to the My Documents folder. The location isn't critical, although you may want to create a standard folder for consistency.
2. Go to **Start** > **Programs** > **Meetinghouse Certificate Installer**. The opening screen is displayed. All valid certificate file types located in the My Documents folder appear in the list.



Valid certificate files in the My Documents folder

3. Tap and hold on a certificate in the list. A pop-up appears asking if you want to install the certificate.
4. Tap **OK**. The certificate is loaded into the correct certificate store.

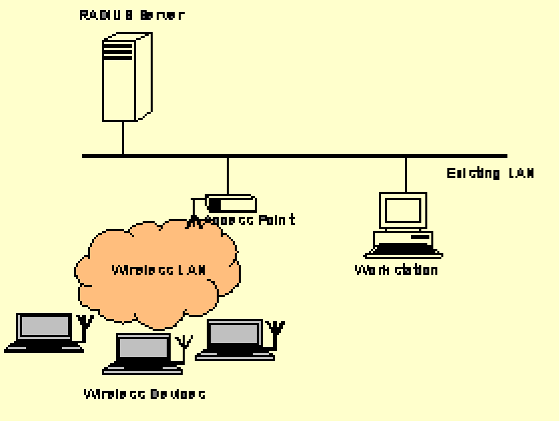
Advice and Workarounds

Issue	Possible Causes and Solutions
The Client will not start on the device with an error message about missing files.	Perform a soft reset.
The wireless network interface (port) does not appear in the main AEGIS screen.	• The license is not valid (If you have entered a time-limited license, is your clock on the device correct?). • Restart the client - on the main screen tap Client > Restart. • Perform a soft reset. • If the radio is turned off or the radio card is not present, this will sometimes cause the port name to not appear. • If the radio driver is very old and does not support NDIS 5.1 commands, the Client may not be able to detect it.
The wireless network interface appears, but when I select it and go to the "configure" menu, the Scan button is disabled.	Power up the radio; see Powering Up Radios on page 4-9.
The client is not attaching to the correct access point.	The **default** network profile instructs the client to attach to the first available access point. You must select a network, move it to the Configured Networks list, and then move it above **default** in the list using the up arrow buttons. For more information, see Wireless Networks Tab on page 9-33.
The Client is failing authentication even though all my information was entered correctly.	1. Verify that the network profile for the access point corresponds to the authentication profile you created for it. • Select the network profile in the Configured Networks list. • Tap **Properties**. The Profile Info tab opens - see page 9-37. • In the Authentication profiles drop-down list, select the profile you want to review. • Tap **View**. The User tab appears displaying the profile’s information. 2. Verify that you have configured the identity and password into the correct fields on the User tab (page 9-37) in the authentication profile. If you are using PEAP or TTLS, the username and password are entered in the Tunneled authentication section.
My Access Point does not broadcast its SSID. Even though I have manually configured an access point with that name, the Client won't associate with it.	• Make sure that the desired SSID is listed as the Network Name, not the Network Profile (which is a screen label) • Verify that Do Active Scan is selected on the Profile Info tab; see Do active scan on page 9-37. Otherwise, the Client will not attempt to find the access point.
I am authenticated, but I don't get an IP address through DHCP.	On the main screen, tap and hold on your access point, tap Configure on the popup menu, and select the Protocol tab. Verify that **Renew IP Address** is selected; see Renew IP address on page 9-35.
I cannot attach to my old network that does not support 802.1x authentication, but is using WEP encryption.	• Verify that you can see your SSID in the Available Networks list on the Wireless Networks tab. Move the SSID to the top of the Configured Networks list so that it is accessed first. If the SSID is not there, you can add it manually and enter the SSID as the network name - page 9-33 • Select the SSID and tap **Properties**. • On the Profile Info tab, select **Do active scan** if your access point does not broadcast its SSID. • On the WEP Mgmt tab, select **Use key for data encryption** and **Use key to authenticate with AP**. • Enter the WEP Key - see Key on page 9-38. • On the Protocol tab, select **Renew IP Address** (unless you have entered one manually separate from the Client) • Note that the port status indicator in the main screen reads "Associated," not "Authenticated" when the connection is complete; although the log file will indicate "Entered AUTHENTICATED state."

Advice and Workarounds

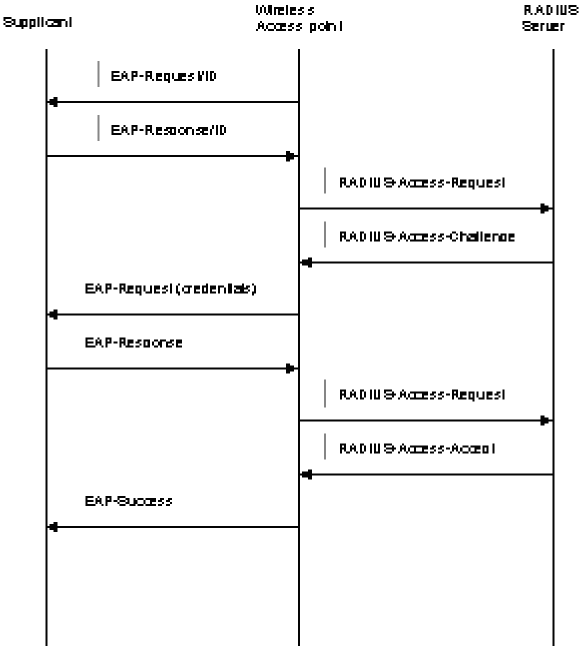
Issue	Possible Causes and Solutions
I made changes, but they do not appear to have taken effect.	Always tap **OK** before exiting a screen you have changed. Then restart the Client from the Client menu on the main screen.
How do I enable peer-to-peer (ad-hoc) mode to have two clients communicate without an access point?	• On the Wireless Networks tab, add a new profile to the Configured Network list. • On the Profile Info tab, give each side the same network name (SSID). • Select **Peer-to-Peer Group (ad hoc mode)** and **Do active scan**. • On the WEP management section, select Use key for data encryption and enter an identical key for both clients. • Verify that this network profile is the first (or only) one in the Configured Network list and try to restart both clients at roughly the same time.

How 802.1X Works



The network elements in the above graphics are those involved in a typical wireless LAN. When 802.1X is running, a wireless device must authenticate itself with the access point in order to get access to the Existing LAN. With respect to the terms used in the 802.1X standard, access points (APs) function as authenticators and wireless devices function as supplicants. The authenticator keeps a control port status for each Client it is serving. If a Client has been authenticated, its control port status is said to be Authorized, and the Client can send application data to the LAN through the AP. Otherwise, the control port status is said to be Unauthorized, and application data cannot traverse the AP.

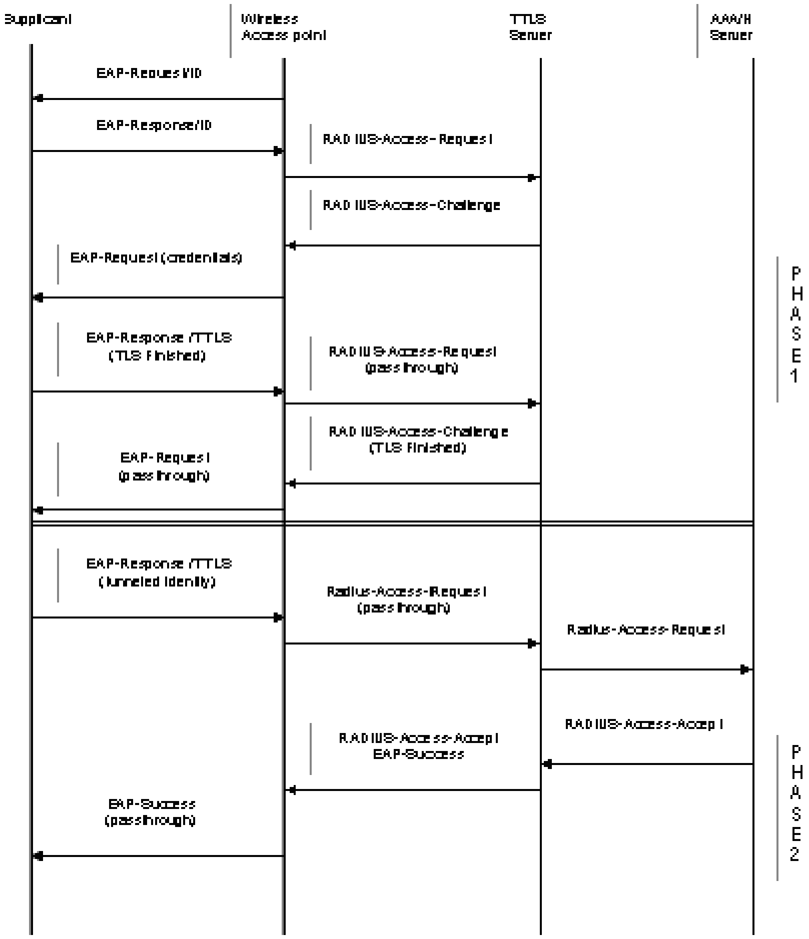
Typical Message Exchange Using MD5 or TLS



The above graphic displays the typical message exchange when the device and the AP support 802.1X. When an AP acting as an authenticator detects a wireless station on the LAN, it sends an EAP-Request for the user's identity to the terminal. In turn, the terminal responds with its identity, and the AP relays this identity to an authentication server, which is typically an external RADIUS server.

The RADIUS server can then act as a central repository of user profile information. Such use of a centralized authentication server allows the user to access wireless LANs at many different points, but still be authenticated against the same server. In response to the Access-Request, the RADIUS server sends an Access-Challenge to the AP, which is then relayed in the form of an EAP-Request to the device. The device sends its credentials to the AP, which in turn relays them to the RADIUS server. The RADIUS server determines whether access to the network is accepted or denied based on the Client's credentials.

Typical Message Exchange Using TTLS and PEAP


Supplicant
Wireless Access point
TTLS Server
AAA/H Server
EAP-Request/ID
EAP-Response/ID
RADIUS-Access-Request
RADIUS-Access-Challenge
EAP-Request (credentials)
EAP-Response /TTLS (TLS Finished)
RADIUS-Access-Request (pass through)
RADIUS-Access-Challenge (TLS Finished)
EAP-Request (pass through)
PHASE 1
EAP-Response /TTLS (tunneled Identity)
Radius-Access-Request (pass through)
Radius-Access-Request
RADIUS-Access-Accept
RADIUS-Access-Accept EAP-Success
EAP-Success (pass through)
PHASE 2

The above graphic shows a typical message flow for a TTLS transaction. TTLS authentication comprises two phases. In Phase 1, TLS is used to authenticate the TTLS server to the client. The TTLS server may optionally request authentication of the client's certificate, but by default the client verifies only the server's certificate. The TLS handshake is negotiated between the client and the TTLS server. Following the TLS handshake, Phase 2 may proceed using a secure channel (tunnel) provided by the TLS record layer. The secure tunnel is then used to exchange information for the negotiation of the following legacy protocols: EAP-MD5, PAP, CHAP, MS-CHAP, or MS-CHAPV2 (subject to support by the AAA server). A TTLS server may perform the authentication, or the information may be de-tunneled and passed on to an AAA server. The AAA server is the server in the user's home domain where authentication and authorization are administered.

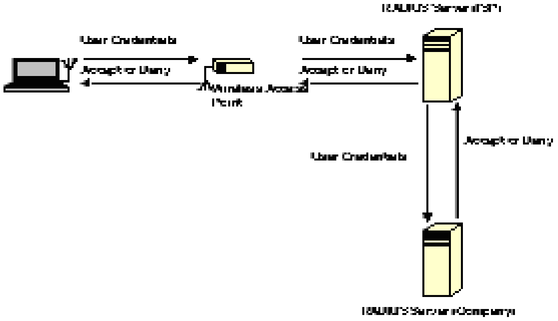
PEAP works in the same manner as TTLS. However, supports different legacy protocols within the encrypted Phase 2 tunnel. Currently the tunneled protocols are EAP-MSChapV2 and EAP-TLS/SmartCard. Like TTLS, the use of a client certificate is optional, if one is used, the same certificate is used for Phase 1 and Phase 2. The client certificate is optional for both phases.

Benefits of 802.1X

Central User Administration

The Client allows network administrators to continue to use RADIUS or another AAA server as their centralized authentication server. In 802.11b, where authentication took place between the access point and the station, there was no concept of passing credentials from the access point to an authentication server. For LANs this was fine. However, as users began to use their devices in remote locations, the security provided became inadequate. 802.1X solves this problem by allowing access points to pass client credentials to the appropriate authentication server.

For example, the following graphic displays the authentication flow for a mobile user who wishes to create a virtual private network with his home office.



By using the Client, the user can associate with a wireless network provided by a third party, in this case the ISP. We assume that the company and the ISP have established a service relationship beforehand. When the ISP receives the user's credentials, the ISP proxies the credentials to the company's AAA server, which returns a message telling the ISP to either accept or deny the user access. This response is then propagated to the remote user.

Dynamic Session Specific Wireless Encryption Keys

There have been many published reports recently about the lack of security provided by the Wired Equivalent Privacy (WEP) protocol. One of the problems with WEP is that the shared key used by the station and the access point is inherently static. That is, this shared key will only change if it is manually reconfigured on both devices. The Client remedies this by supporting the Transport Layer Security (TLS) protocol. TLS ensures that a new shared key is generated each time a station associates itself with an access point. TLS has proven itself an excellent authentication and encryption protocol in commercial environments. The Client also supports the MD5 and TTLS security protocols.

Additional Advantages of TTLS and PEAP

The Client provides the advantage of Tunneled TLS (TTLS) and PEAP support. These protocols provide the security of TLS with greatly reduced administrative load. Security is enhanced by never passing user ID and password in the clear. No "real" user ID or password is required in Phase 1. After the secure tunnel is established, Phase 2, user credentials are passed in safe, encrypted form. To further enhance security, the WEP keys, which encrypt the data between the wireless card and the AP, may be automatically changed on a per-session basis, limiting the time available to an unauthorized sniffer to crack the keys. By limiting the session time (the reauthentication period), the keys can essentially be made uncrackable.

Administration is eased by greatly reduced certificate requirements in comparison to TLS. In TLS, each client must have a client certificate to pass to the server, and a CA certificate with which to verify a server certificate, while the server must have a client certificate from each user and CA certificates for each possible CA chain and its own server certificate. TTLS and PEAP require only that a single server certificate be created for the server to present to the client, and that the client have a CA certificate to verify the server. Because these are the same for each client on the network, they are easily managed, unlike TLS, where every client certificate is unique. TTLS and PEAP thus provide the security of a TLS channel without the need for managers to distribute and manage client certificates. Lastly, TTLS allows for the use of existing legacy authentication protocols. Administrators may continue to use established authentication databases.

Cisco LEAP

The message exchange used by Cisco LEAP is proprietary. This protocol is not a standard EAP type, but is supported by the Client through a licensing arrangement with Cisco.

Relative Merits of Authentication Protocols

MD5 is the least secure of the EAP protocols as it only does a one-way authentication, and does not support automatic distribution and rotation of WEP keys, increasing the administrative burden of manual WEP key maintenance.

TLS, while the most secure EAP protocol, requires client certificates to be installed on each wireless client. Establishing and maintaining this PKI infrastructure is normally a burden most administrators do not feel is worth the extra level of security gained.

TTLS and PEAP bypassed the certificate issue by tunneling TLS, and thus eliminating the need for a certificate on the client side. PEAP supports only EAP-compliant authentication protocols within the tunnel structure, and is rapidly becoming the most widely supported of the EAP methods. TTLS supports pre-EAP authentication protocols within the tunnel structure, and should be used in those circumstances when pre-EAP interior protocols are desirable.

LEAP is a pre-EAP, Cisco-proprietary protocol, with many of the features of EAP protocols. Cisco controls the ability of other vendors to implement this protocol, so it should be selected for use only when limited vendor choice for client, access-point, and server products is not a concern.

Differences Between Protocols

Security Feature	**MD5 Challenge**	**TLS**	**TTLS**	**PEAP**	**LEAP**
Client -side certificate required?	No	Yes	No	No	No
Server-side certificate required?	No	Yes	No	Yes	No
Dynamic WEP Re-keying	No	Yes	Yes	Yes	Yes
Mutual or One-way Authentication?	One-way	Mutual	Mutual	Mutual	Mutual
Support of non-EAP protocols within a secure tunnel?	N/A	N/A	Yes	No	N/A
Relative Deployment Complexity	Simple	Difficult	Moderate	Moderate	Moderate
Relative Security	Poorest	Highest	High	High	High

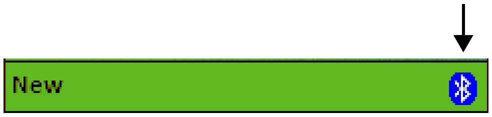
10 Wireless PAN Communications with Bluetooth

Overview

Dolphin 7900 terminals are available with a Bluetooth radio for WPAN (Wireless Personal Area Network) usage. When the mobile computer is first initialized, the *.cab file and module for Bluetooth are installed.

Powering Up the Bluetooth Radio Driver

Before using the radio, make sure that the Bluetooth radio is powered up. When the radio driver is powered up, the Bluetooth icon appears in the task tray on the Today screen.

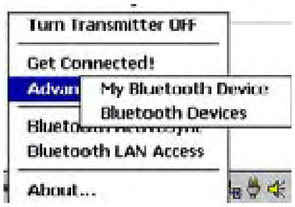


Radios are powered up in the Radio Manager utility; see Powering Up Radios on page 4-9.

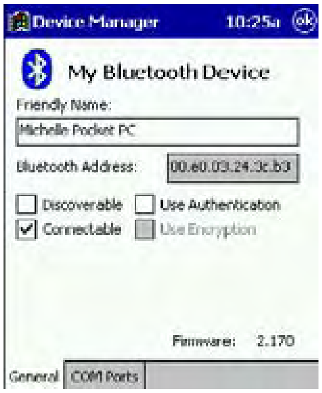
Setting Up Your Bluetooth Card

Note: If you use the Get Connected! Wizard, which is recommended for normal usage, then this step is not necessary. This step would be used to change the friendly name of your mobile computer.

1. Tap the Bluetooth icon that appears in the task tray on the Today screen.
2. In the pop-up menu, select **Advanced Features**, then **My Bluetooth Device**. (If you installed OBEX, the menu also lists Transfer via Bluetooth.)



3. In the **My Bluetooth Device** screen, you can modify the **Friendly Name** and make any desired configuration changes. When done, tap **OK**.



Friendly Name: Michelle Pocket PC

Bluetooth Address: 00.e0.03.24.3c.b3

□ Discoverable □ Use Authentication

☑ Connectable □ Use Encryption

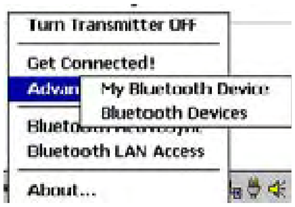
Firmware: 2.170

- In normal phone connect operation, **Discoverable** mode is not needed and should be disabled.
- If you do enable **Discoverable** mode (e.g., for ActiveSync), note that it does not shut off by itself. To save power, remember to disable it when not needed.
- **Connectable**, **Use Authentication**, and **Use Encryption** are also not required for printing or dial-up networking applications.
- Check Use **Authentication** to enable the **Use Encryption** option.

Assign COM Ports

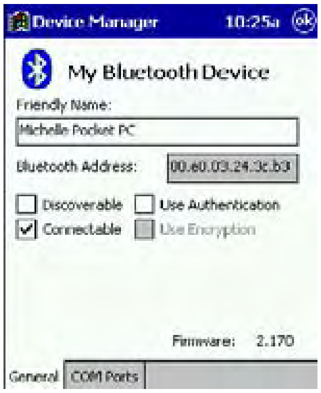
Follow these steps to view and/or modify the Bluetooth COM ports. If you are not going to use the IrDA port, you can disable it to free up a port for Bluetooth devices; see Using Infrared on page 8-6.

1. Tap on the Bluetooth icon on the Today screen. Select **Advanced Features** then **My Bluetooth Device**.



Note: If you installed OBEX, the menu also lists Transfer via Bluetooth.

2. The **My Bluetooth Device** screen appears. Tap on the **COM Ports** tab.



My Bluetooth Device

Friendly Name: Michelle Pocket PC

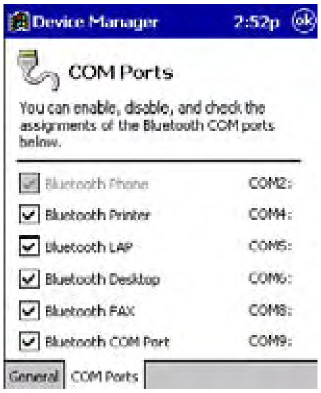
Bluetooth Address: 00.e0.03.24.3c.b3

□ Discoverable □ Use Authentication

☑ Connectable □ Use Encryption

Firmware: 2.170

3. As needed, view and/or enable/disable the Bluetooth COM port assignments. Tap **OK**.



COM Ports

You can enable, disable, and check the assignments of the Bluetooth COM ports below.

☑ Bluetooth Phone COM2:

☑ Bluetooth Printer COM4:

☑ Bluetooth LAP COM5:

☑ Bluetooth Desktop COM6:

☑ Bluetooth FAX COM8:

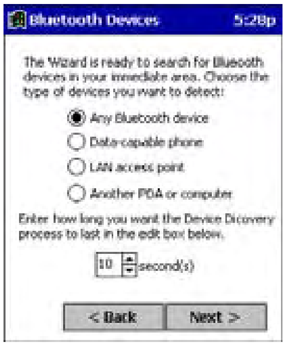
☑ Bluetooth COM Port COM9:

Note: The Bluetooth Phone port cannot be disabled. For more information about COM ports, see Com Port Assignment Table on page 7-21.

Discover Bluetooth Device(s)

Follow these steps to discover other Bluetooth devices nearby, including non-phone devices. The Device Discovery Wizard is a more detailed alternative to using the Bluetooth "Get Connected!" Wizard or Bluetooth ActiveSync or Bluetooth LAN Access options. The Device Discovery Wizard allows you to discover any type of Bluetooth device.

1. If not open, launch the **Bluetooth Devices** folder. Tap on the Bluetooth icon on the **Today** screen. Select **Advanced Features** then **Bluetooth Devices**.
2. In the **Bluetooth Devices Folder**, tap on the **Device Discovery** icon. Or you can tap on **Tools**. In the pop-up menu, select Device Discovery.
3. Follow the Bluetooth Device Discovery Wizard to search for Bluetooth devices nearby. When prompted, select the device type you seek.



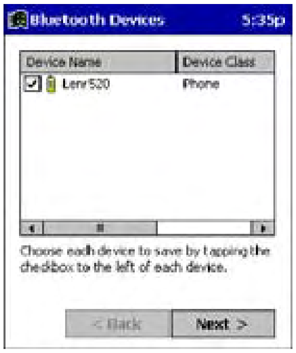
The Wizard is ready to search for Bluetooth devices in your immediate area. Choose the type of devices you want to detect:

● Any Bluetooth device
○ Data-capable phone
○ LAN access point
○ Another PDA or computer

Enter how long you want the Device Discovery process to last in the edit box below.

10 second(s)

4. When the search is complete, a screen reports the discovered Bluetooth devices. Check the box next to any device you wish to save information about, (i.e., any devices you wish to connect to). Tap **Next**.



Device Name	Device Class
☑ Lenr520	Phone

Choose each device to save by tapping the checkbox to the left of each device.

5. A service discovery phase begins, 5-10 seconds per chosen device.
6. In the next screen, tap **Finish**.

Bond With Discovered Device(s)

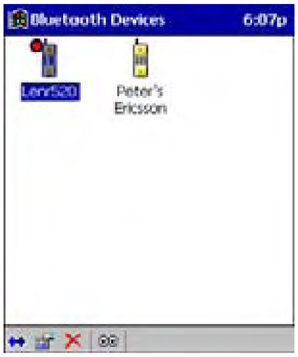
Follow these steps to bond with an already discovered Bluetooth device. In most cases, bonding is for establishing secure communications with a Bluetooth-enabled phone. This is a more detailed alternative to using the Bluetooth "Get Connected! Wizard."

Important!

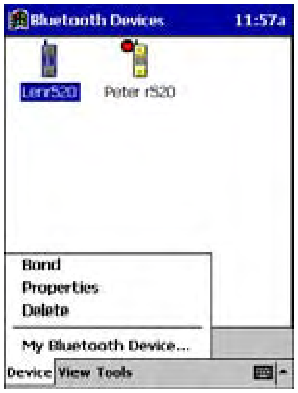
- Do not try to bond with a Motorola Timeport 270C or Nokia 6310!
- Do not use this method to bond with a printer! The third-party printing software included on the installation CD also handles bonding.

1. If not open, launch the **Bluetooth Devices** folder. Tap on the Bluetooth icon in the Today screen. Select **Advanced Features,** then **Bluetooth Devices**.

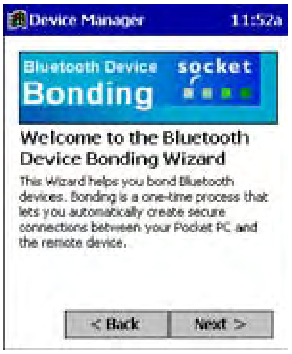
2. Tap and hold your stylus on the Bluetooth device you want to bond with. In the pop-up menu, select **Bond**.



3. Alternatively, after selecting a device, tap on the **Bond** icon. Or tap on **Device**, then select **Bond**.



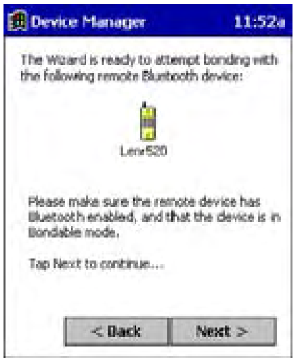
4. The **Bluetooth Device Bonding Wizard** launches. Follow the wizard to bond with your selected device.



Welcome to the Bluetooth Device Bonding Wizard

This Wizard helps you bond Bluetooth devices. Bonding is a one-time process that lets you automatically create secure connections between your Pocket PC and the remote device.

5. As prompted, make sure the Bluetooth device that you want to bond with is in *Bondable* mode.



Device Manager 11:52a

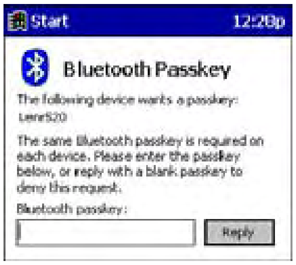
The Wizard is ready to attempt bonding with the following remote Bluetooth device:

Lenr520

Please make sure the remote device has Bluetooth enabled, and that the device is in Bondable mode.

Tap Next to continue...

6. If the remote device is set up to accept bonding, a **Bluetooth Passkey** screen appears. To continue bonding, enter the correct passkey and tap **Reply**.



Start 12:28p

Bluetooth Passkey

The following device wants a passkey:
Lenr520

The same Bluetooth passkey is required on each device. Please enter the passkey below, or reply with a blank passkey to deny this request.

Bluetooth passkey:

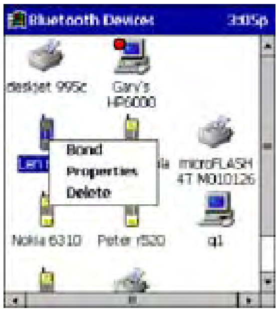
7. When you have successfully bonded with the other device, tap **Finish**.

View Device Properties

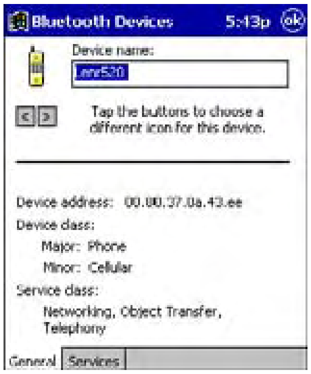
Follow these steps to view the properties of an already discovered device.

1. If not open, launch the **Bluetooth Devices** folder. Tap on the Bluetooth icon on the Today screen. Select **Advanced Features** then **Bluetooth Devices**.

2. Select a device. Tap on the **Properties** icon, or tap on **Device** then select **Properties**. Alternatively, you can tap and hold your stylus on the Bluetooth device you want to view information about. In the pop-up menu, select **Properties**.



3. Use the **General** and **Services** screens to research device properties. If needed, assign a new device type icon by tapping on the arrow buttons in the **General** screen. You can also use the **Device name** field to rename the device. When done, tap **OK** for the setting to take effect.



Device name: Lmr520

Tap the buttons to choose a different icon for this device.

Device address: 00.80.37.0a.43.ee

Device class:

Major: Phone

Minor: Cellular

Service class:

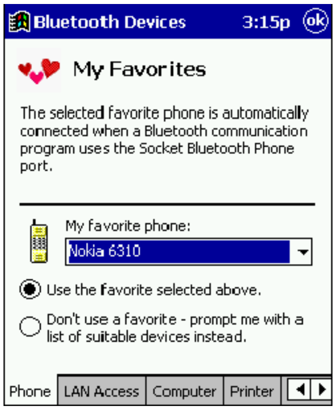
Networking, Object Transfer, Telephony

Set Up Your Favorite Device

Follow these steps to set up default devices in the **Bluetooth Devices** folder. Please note that the Get Connected! Wizard automatically assigns the favorite phone.

Complete these steps:

1. Tap on **Tools** and select **My Favorites**.
2. Tap on the tab for the type of device you would like to set a favorite for. If needed, use the arrow buttons to scroll and find the tab you need.



My Favorites

The selected favorite phone is automatically connected when a Bluetooth communication program uses the Socket Bluetooth Phone port.

My favorite phone: Nokia 6310

● Use the favorite selected above.

○ Don't use a favorite - prompt me with a list of suitable devices instead.

Note: Tabs appears only for COM ports you have enabled. To enable a port, refer to the “Assign COM Ports” section earlier in this chapter.

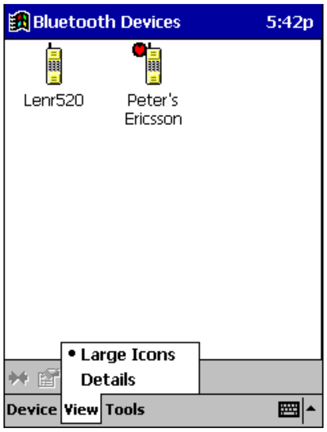
3. To select a favorite device, select **Use the favorite selected above**. In the drop-down list, select your device. Tap **OK**.
4. After setting a device as your favorite, its icon appears in the Bluetooth Devices folder with a heart next to it.

Change Views

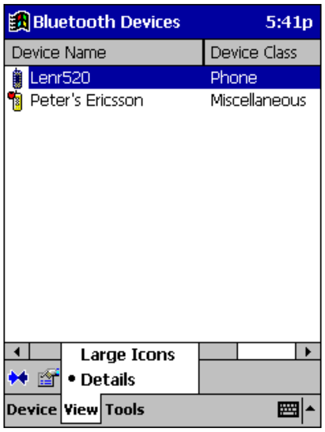
You can switch between the **Large Icons** or **Details** views for the **Bluetooth Devices** folder.

1. In Bluetooth Devices, tap on **View**.

2. In the pop-up menu, choose between **Large Icons** or **Details**.



Large Icons



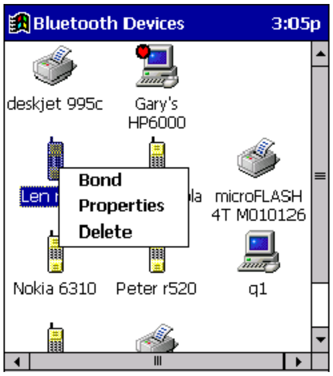
Details

Note: In Details view, you can see the Device Class and scroll right to see the current Bonded status.

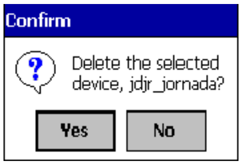
Delete a Device From the Folder

If you no longer plan to connect with it, you can delete a device from the **Bluetooth Devices** folder.

1. If not open, launch the **Bluetooth Devices** folder.
2. Tap and hold your stylus on the device you wish to delete. In the pop-up menu, select **Delete**.



3. Alternatively, after selecting a device, tap on the **Delete** icon. Or tap on **Device** then select **Delete**.
4. A Confirm screen appears. Tap **Yes**.

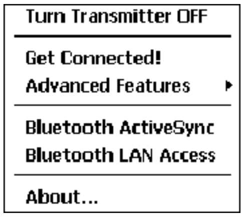


Delete the selected device, jdjr_jornada?

Turn Radio Transmitter ON/OFF

You may want to turn off the radio transmitter to save power or if you are entering an area with radio restrictions (e.g., an airplane).

1. The Bluetooth icon should appear in the task tray on the **Today** screen. Tap on the icon.
2. In the pop-up menu, select **Turn Transmitter OFF**.

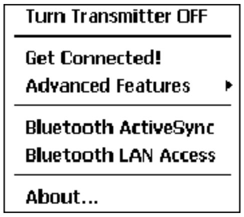


3. The Bluetooth Card radio transmitter shuts off. The Bluetooth icon in the task tray becomes gray, as well as relevant menu options (e.g., Get Connected!).
4. To turn the radio transmitter back on, tap on the gray **Bluetooth** icon. In the pop-up-menu, select **Turn Transmitter ON.**

Bluetooth ActiveSync

This section explains how to use the Bluetooth ActiveSync feature. It helps you quickly and easily ActiveSync to a notebook or desktop computer with ActiveSync v3.x installed.

1. Tap on the **Bluetooth** icon. In the pop-up menu, select **Bluetooth ActiveSync**.

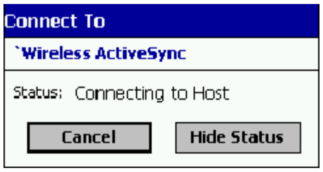


2. The next screens varies depending on if your Bluetooth Devices folder contains any computers, and if one is chosen as your favorite. Please refer to the appropriate scenario:

SCENARIO #1: Your Bluetooth Devices folder contains a favorite desktop computer.

(a) When you tap **Bluetooth ActiveSync**, your mobile computer automatically tries to connect to your favorite computer.

(b) The Connect To screen appears, reporting that it is trying to connect to Wireless ActiveSync.


Connect To

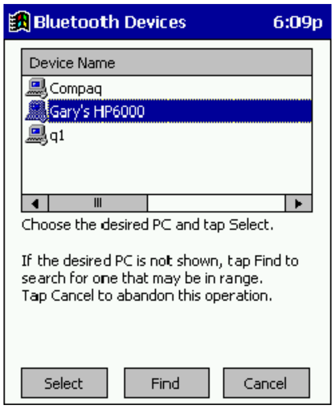
`Wireless ActiveSync

Status: Connecting to Host

(c) After a successful connection is made, the status screen reports Connected. Now you are ready to synchronize files, if desired.

SCENARIO #2: Your Bluetooth Devices folder contains no favorite desktop computer.

(a) When you tap on **Bluetooth ActiveSync**, a screen appears that allows you to choose which computer to connect to in your Bluetooth Devices folder. Choose a computer from the list and tap Select, or tap **Find** to search for another computer.


Bluetooth Devices 6:09p

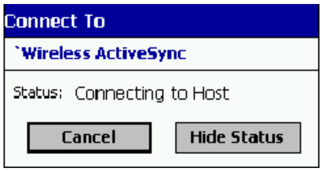
Device Name
Compaq
Gary's HP6000
q1

Choose the desired PC and tap Select.

If the desired PC is not shown, tap Find to search for one that may be in range.
Tap Cancel to abandon this operation.

Note: If the computer you want to connect to is not listed, tap **Find** to begin a search. Proceed as described in Scenario #3 on page 10-10.

(b) Your mobile computer attempts to connect to your selected computer.

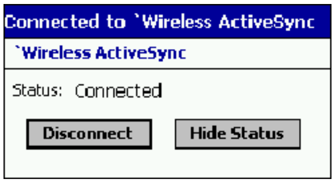


Connect To

`Wireless ActiveSync

Status: Connecting to Host

(c) After a successful connection is made, the status screen reports Connected. Now you are ready to synchronize files, if desired.



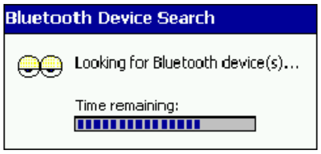
Connected to `Wireless ActiveSync

`Wireless ActiveSync

Status: Connected

SCENARIO #3: Your Bluetooth Devices folder contains no computers.

(a) When you tap on **Bluetooth ActiveSync**, a Bluetooth Device Search automatically begins.



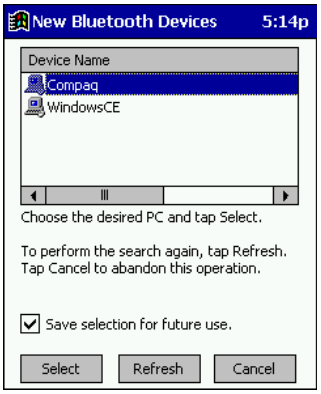
Bluetooth Device Search

Looking for Bluetooth device(s)...

Time remaining:

Note: You can also start the device search by tapping Find in the Bluetooth Devices screen.

(b) After the search is complete, select the computer you wish to ActiveSync with and tap **Select**. If the computer is not listed, make sure the computer is discoverable and tap **Refresh** to search again.



New Bluetooth Devices 5:14p

Device Name
Compaq
WindowsCE

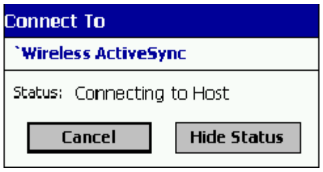
Choose the desired PC and tap Select.

To perform the search again, tap Refresh.
Tap Cancel to abandon this operation.

☑ Save selection for future use.

(c) After you tap **Select**, a service discovery phase begins.

(d) The Connect To screen appears, reporting that it is trying to connect to Wireless ActiveSync.



Connect To

`Wireless ActiveSync

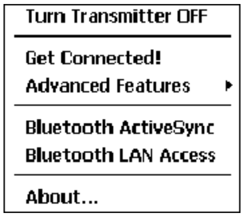
Status: Connecting to Host

(e) After a successful connection is made, the status screen reports Connected. Now you are ready to synchronize, if desired.

Bluetooth LAN Access

This section explains how to use the Bluetooth LAN Access feature to quickly and easily connect to a Bluetooth-enabled LAN access point.

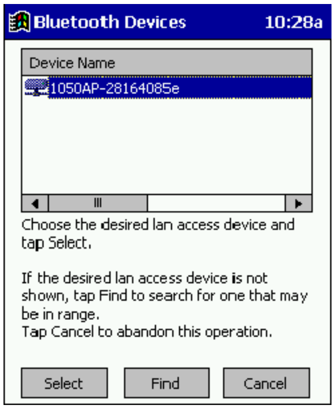
1. Tap on the **Bluetooth** icon. In the pop-up menu, select **Bluetooth LAN Access**.



2. The next screens varies depending on if your Bluetooth Devices folder contains any access points, and if one is chosen as your favorite. Please refer to the appropriate scenario:

SCENARIO #1: Your Bluetooth Devices folder contains no favorite access point.

(a) When you tap Bluetooth LAN Access, a screen appears that allows you to choose which access point to connect to in your Bluetooth Devices folder. Choose an access point from the list and tap **Select**.

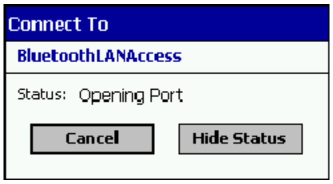


Choose the desired lan access device and tap Select.

If the desired lan access device is not shown, tap Find to search for one that may be in range.
Tap Cancel to abandon this operation.

Note: If your access point is not listed, tap Find and proceed as described in Scenario #3.

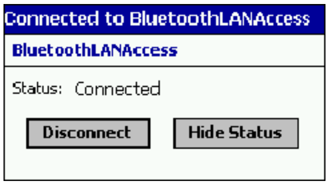
(b) Your mobile computer tries to connect to the selected access point.



Status: Opening Port

(c) If your LAN requires a passkey, a screen appears asking for the passkey. Enter the passkey, then tap **OK**.

(d) After a successful connection is made, the status screen reports Connected.

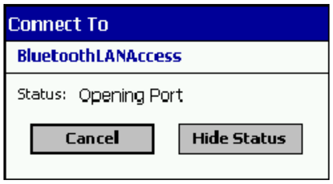


Status: Connected

(e) Now you are ready to access your LAN for Internet access, files, etc.

SCENARIO #2: Your Bluetooth Devices folder contains a favorite access point.

(a) When you tap **Bluetooth LAN Access**, your mobile computer automatically tries to connect with your favorite access point.



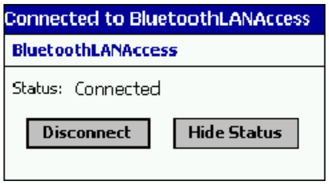
Connect To

BluetoothLANAccess

Status: Opening Port

(b) If your LAN requires a passkey, a screen appears, asking for the passkey. Enter the passkey, then tap **OK**.

(c) After a successful connection is made, the status screen reports Connected.



Connected to BluetoothLANAccess

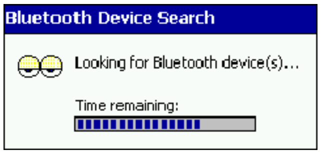
BluetoothLANAccess

Status: Connected

(d) Now you are ready to access your LAN for Internet access, files, etc.

SCENARIO #3: Your Bluetooth Devices folder has no access points.

(a) When you tap **Bluetooth LAN Access**, the mobile computer automatically begins to search for new Bluetooth devices.



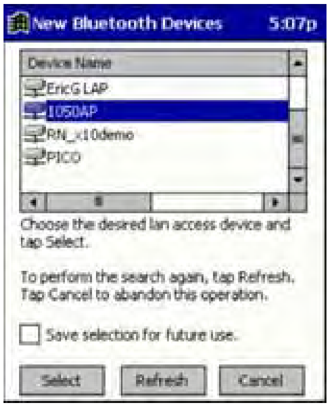
Bluetooth Device Search

Looking for Bluetooth device(s)...

Time remaining:

Note: You can also start the device search by tapping Find in the Bluetooth Devices screen. See Scenario #2 on page 10-9.

(b) After the search is complete, select the access point you wish to connect to. Tap **Select**. If the access point is not listed, tap **Refresh** to search again.



New Bluetooth Devices 5:07p

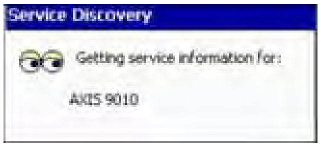
Device Name
EricG LAP
1050AP
RN_x10demo
PICO

Choose the desired lan access device and tap Select.

To perform the search again, tap Refresh. Tap Cancel to abandon this operation.

□ Save selection for future use.

(c) After you tap **Select**, a service discovery phase begins.



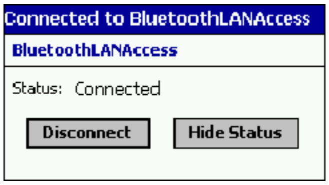
Service Discovery

Getting service information for:

AXIS 9010

(d) If the LAN requires a Passkey, a screen appears, asking for the Passkey. Enter the passkey, then tap **OK**.

(e) After a successful connection is made, the screen reports Connected.



Connected to BluetoothLANAccess

BluetoothLANAccess

Status: Connected

(f) Now you are ready to access your LAN for Internet access, files, etc.

OBEX

This section explains how to use the OBEX (object exchange) application to trade business cards, contacts or files with another Bluetooth device that supports OBEX.

Bluetooth OBEX application supports five operations:

- Exchange Business Cards
- Send a Contact
- Send a File
- Browse Remote Device
- Receive Contact or File
- Enable File Sharing

The first four operations - exchange business cards, send a contact, send a file, and browse remote device - are client-oriented. They involve initiating an object exchange.

The last two operations - receive contact or file and enable file sharing - are server-oriented. They involve accepting objects in an exchange initiated by another Bluetooth device.

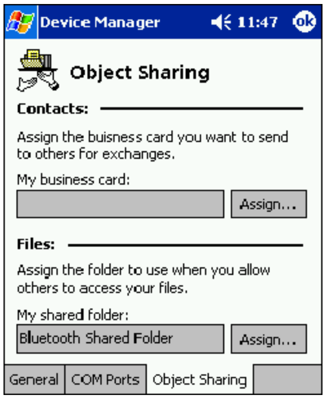
Exchange Business Cards

1. Make sure both Bluetooth devices have a business card assigned to them.

Note: If each device does not have a business card assigned to it, you cannot exchange business cards.

To assign a business card to your mobile computer, do the following:

- Tap on the **Bluetooth** icon. In the pop-up menu, tap **Advanced Features** > **My Bluetooth Device**.
- Tap on the **Object Sharing** tab. Under My business card, tap **Assign**



Object Sharing

Contacts:

Assign the buisness card you want to send to others for exchanges.

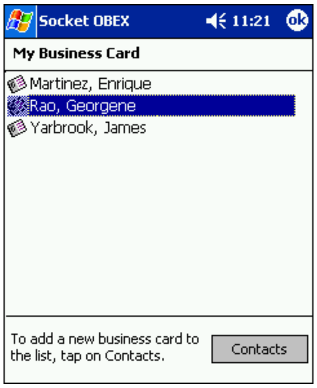
My business card:

Files:

Assign the folder to use when you allow others to access your files.

My shared folder: Bluetooth Shared Folder

- In the next screen, select your business card and tap **OK**. If your business card is not listed, tap **Contacts** to create one.



My Business Card

Martinez, Enrique
Rao, Georgene
Yarbrook, James

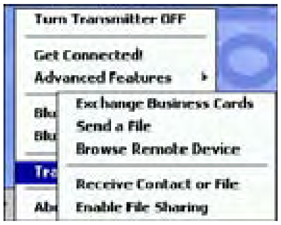
To add a new business card to the list, tap on Contacts.

When you return to the Object Sharing screen, tap **OK**.

2. Make sure the other Bluetooth device is set up to receive a contact. The device must support the OBEX Object Push profile.

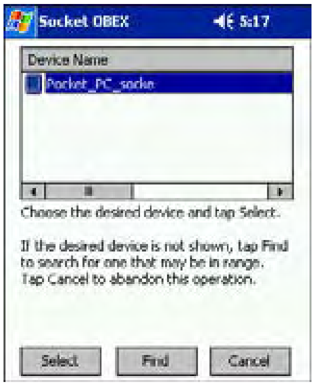
Note: If the other device is also using the Bluetooth Connection Kit, you can set it up to receive a contact by tapping the **Bluetooth** icon. In the pop-up menu, tap **Transfer via Bluetooth** > **Receive Contact or File**.

3. Now you are ready to exchange business cards. Tap on the **Bluetooth** icon. In the pop-up menu, tap **Transfer via Bluetooth** > **Exchange Business Cards**.



4. If your mobile computer has no devices in the Bluetooth Devices Folder, then it begins to search for Bluetooth devices nearby.

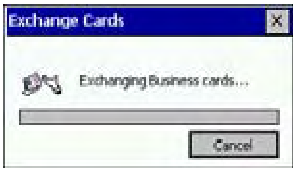
5. Select the Bluetooth device you wish to exchange business cards with. If the device is not listed, tap **Find**.



Choose the desired device and tap Select.

If the desired device is not shown, tap Find to search for one that may be in range. Tap Cancel to abandon this operation.

6. Your mobile computer begins to exchange business cards. After the exchange, the new business card should appear in your Contacts list.



Exchanging Business cards...

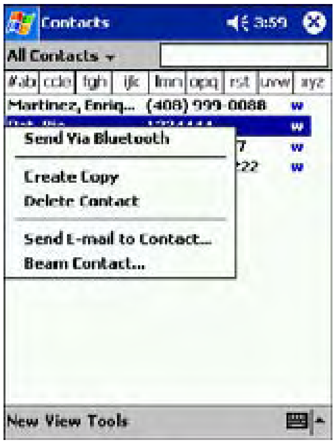
Send a Contact

1. Make sure the other Bluetooth device is set up to receive a contact. It must support the OBEX Object Push server profile. Refer to the documentation that came with the device for instructions.

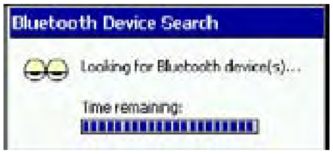
Note: If the other device is also using the Bluetooth Connection Kit, you can set it up to receive a contact by tapping the **Bluetooth** icon. In the pop-up menu, tap **Transfer via Bluetooth** > **Receive Contact or File**.

2. Now you are ready to send a contact. Go to your Contacts folder.

3. Tap and hold your stylus on the contact(s) you would like to send. In the pop-up menu, select **Send Via Bluetooth**.



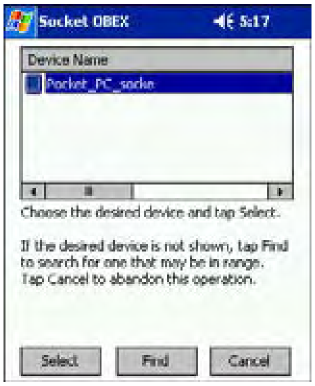
4. If your mobile computer has no devices in the Bluetooth Devices Folder, then it begins to search for Bluetooth devices nearby.


Bluetooth Device Search

Looking for Bluetooth device(s)...

Time remaining:

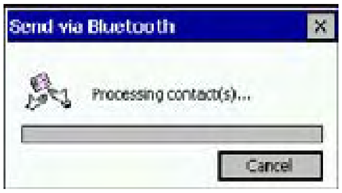
5. Select the Bluetooth device you wish to send the contact(s) to. If the desired device is not listed, tap **Find**.



Choose the desired device and tap Select.

If the desired device is not shown, tap Find to search for one that may be in range. Tap Cancel to abandon this operation.

6. Your mobile computer processes and send the contact(s).


Send via Bluetooth

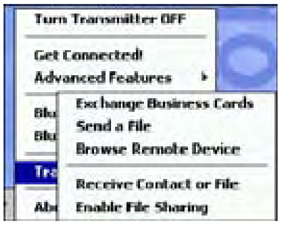
Processing contact(s)...

Send a File

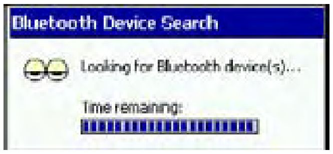
1. Make sure the other Bluetooth device is set up to receive a file. It must support the OBEX Object Push server profile. Refer to the documentation that came with the device for instructions.

Note: If the other device is also using the Bluetooth Connection Kit, you can set it up to receive a file by tapping the **Bluetooth** icon. In the pop-up menu, tap **Transfer via Bluetooth** > **Receive Contact or File**.

2. Now you are ready to send a file. Tap on the **Bluetooth** icon. In the pop-up menu, tap **Transfer via Bluetooth** > **Send a File**.



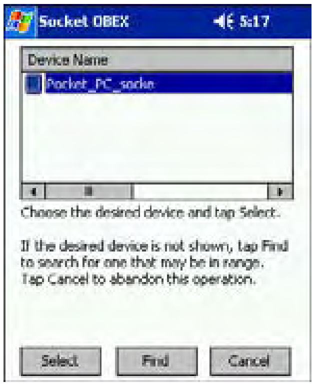
3. If your mobile computer has no devices in the Bluetooth Devices Folder, then it begins to search for Bluetooth devices nearby.


Bluetooth Device Search

Looking for Bluetooth device(s)...

Time remaining:

4. Select the Bluetooth device you wish to send a file. If the desired device is not listed, tap **Find**.

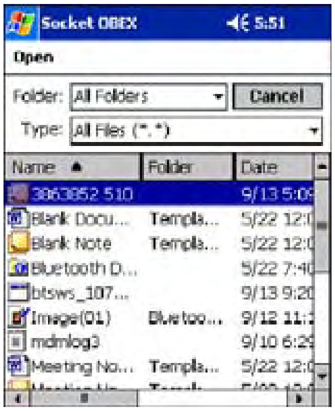


Pocket_PC_socke

Choose the desired device and tap Select.

If the desired device is not shown, tap Find to search for one that may be in range. Tap Cancel to abandon this operation.

5. In the next screen, tap on the file you wish to send. You can use the **Folder** and **Type** drop-down menus to search for your file. Also, you can scroll horizontally to view the folder, date, size, type, and location of each file.

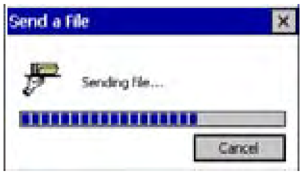


Folder: All Folders

Type: All Files (*.*)

Name ▲	Folder	Date
3863852 510		9/13 5:0
Blank Docu...	Templa...	5/22 12:0
Blank Note	Templa...	5/22 12:0
Bluetooth D...		5/22 7:40
btsws_107...		9/13 9:20
Image(01)	Bluetoo...	9/12 11:1
mdmlog3		9/10 6:29
Meeting No...	Templa...	5/22 12:0

6. Your mobile computer sends the file.



Sending file...

Browse Remote Device

The Bluetooth File Explorer lets your mobile computer share files with another Bluetooth device. The other device must support the OBEX File Transfer server profile.

This section covers the following file transfer operations:

- Prepare for file transfer
- Send/receive file(s) or folder(s)
- Create a folder
- Delete file(s) or folder(s)
- Refresh remote view
- Connect/disconnect
- Exit the program

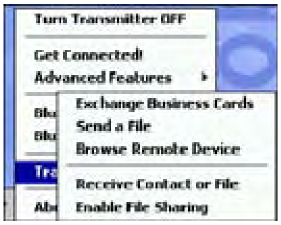
Note: “Local device” refers to the mobile computer you are running the OBEX from. “Remote device” refers to the Bluetooth device you are trying to transfer files with.

Prepare for File Transfer

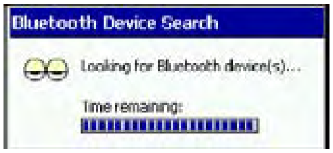
1. Make sure the remote device has file sharing enabled. It must support the OBEX File Transfer server profile.

Note: If the other device is also using the Bluetooth Connection Kit, you can enable file sharing by tapping the **Bluetooth** icon. In the pop-up menu, tap **Transfer via Bluetooth** > **Enable File Sharing**.

2. Now you are ready to browse the remote device. Tap on the **Bluetooth** icon. In the pop-up menu, tap **Transfer via Bluetooth** > **Browse Remote Device**.



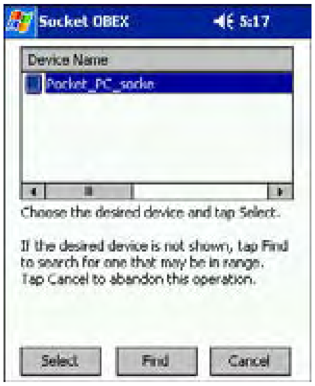
3. If your mobile computer has no devices in the Bluetooth Devices Folder that supports OBEX File Transfer, then it begins to search for Bluetooth devices nearby.



Looking for Bluetooth device(s)...

Time remaining:

4. Select the Bluetooth device you wish to browse. If the desired device is not listed, tap **Find**.

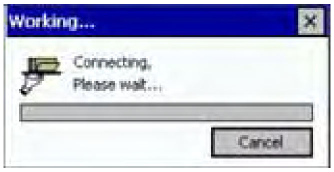


Device Name
Pocket_PC_socke

Choose the desired device and tap Select.

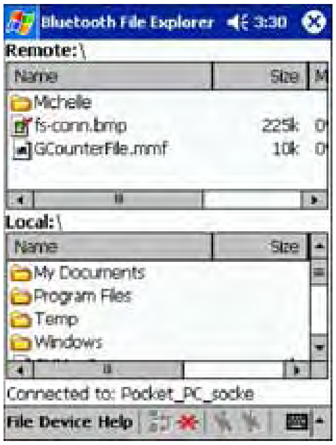
If the desired device is not shown, tap Find to search for one that may be in range.
Tap Cancel to abandon this operation.

5. Your mobile computer begins to establish a file sharing connection.



Connecting,
Please wait...

6. After the devices successfully connect, the Bluetooth File Explorer appears. Half of the screen shows contents of the remote device, while the other half shows contents of your device (the local device). The very bottom of the screen reports the connection status.



Remote:\

Name	Size	M
Michelle		
fs-conn.bmp	225k	0
GCounterFile.mmf	10k	0

Local:\

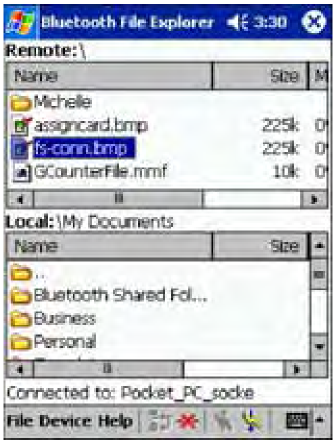
Name	Size
My Documents	
Program Files	
Temp	
Windows	

Connected to: Pocket_PC_socke

Send/Receive File(s) or Folder(s)

- Single-tap items to select them for transfer.
- Double-tap on a folders to open it and see its contents.

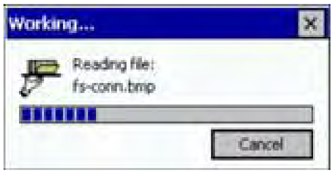
1. Select the file(s) or folder(s) that you wish to transfer. You can select items from only one device per transfer session.



2. There are two different ways to initiate the transfer:

- Tap on the **File** menu. Select **Send to remote** or **Get from remote**, as applicable. The inappropriate option should be gray.
- Tap on the **Send to remote** icon or **Get from remote** icon, as applicable. The inappropriate icon should be gray.

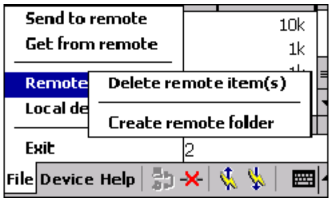
3. A screen reports the status of the transfer.



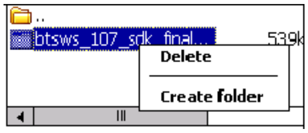
4. After the transfer, a copy of each selected item should appear in the other device.

Create a Folder

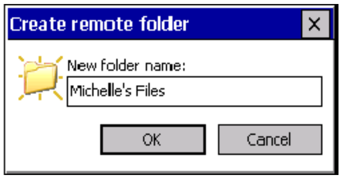
1. Tap on the **File** menu. Select **Remote device** or **Local device**, wherever you want to create a folder, then tap **Create remote folder** or **Create local folder**, as applicable.



2. You can also tap and hold your stylus on an item in either the remote or local device that you wish to put in a new folder. In the pop-up menu, select **Create folder**.



3. In the next screen, enter a name for your new folder. Tap **OK**.

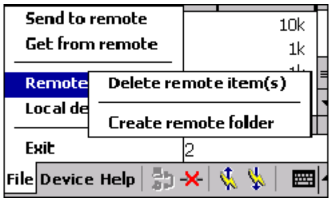


New folder name: Michelle's Files

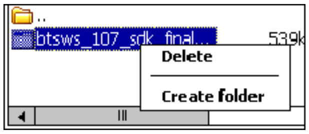
4. The new folder should be listed under the appropriate device.

Delete File(s) or Folder(s)

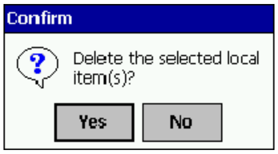
1. Select item(s) that you wish to delete. You can only delete item(s) from one device at a time.
2. Tap on the **File** menu. Select **Remote device** or **Local device**, wherever the item(s) are located, then tap **Delete remote item(s)** or **Delete local item(s)**, as applicable.



3. Tap and hold your stylus an item in either the remote or local device that you wish to put in a new folder. In the pop-up menu, select **Delete folder**.



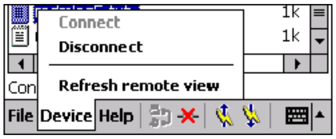
4. In the Confirm screen, tap **Yes**.



Delete the selected local item(s)?

Refresh Remote View

1. Tap on the **Device** menu. Select **Refresh** remote view.



2. Your local device begins to read the contents of the remote device.
3. After a few seconds, the contents view of the remote device is refreshed.

Connect/Disconnect

To connect to the remote device, do the following:

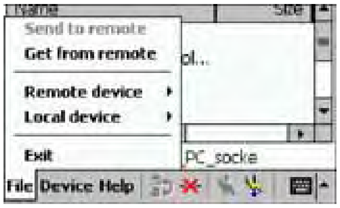
1. Make sure the remote device has file sharing enabled.
2. Start the connection process by either of two methods:
   - Tap on the Device menu. Select Connect.
   - Tap on the Connect icon.
3. In the next screen, select the device you wish to connect to. Tap **Select**. Your mobile computer attempts to connect to the device selected.

To disconnect from the remote device, do the following:

1. Start the disconnection process by either of two methods:
   - Tap on the **Device** menu. Select **Disconnect**.
   - Tap on the **Connect** icon.
2. Your mobile computer disconnects from the remote device. Afterwards, no contents are listed for the remote device.

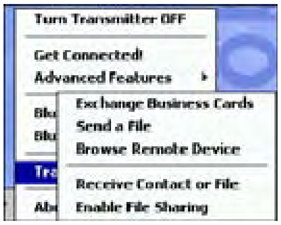
Exit Bluetooth File Explorer

To exit the Bluetooth File Explorer, tap **File** > **Exit**.

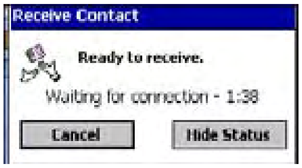


Receive Contact or File

1. Tap on the **Bluetooth** icon. In the pop-up menu, tap **Transfer via Bluetooth** > **Receive Contact or File**.



2. The Receive Contact or File status screen appears. Your mobile computer waits two minutes for the contact or file.



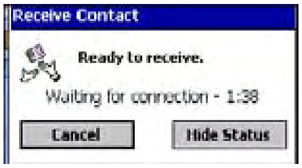
Ready to receive.

Waiting for connection - 1:38

3. After successfully connecting to the remote device, the screen reports Connected then disappear. The new contact or file should now be on your device.
4. If two minutes passes before you receive the item, tap **Wait Again**.
5. After you receive the file or contact, the “Receive Contact or File” feature is automatically disabled.

Enable File Sharing

1. Tap on the **Bluetooth** icon. In the pop-up menu, tap Transfer via **Bluetooth** > **Enable File Sharing**.
2. The Enable File Sharing status screen appears. Your mobile computer waits two minutes for the remote device to connect.


Receive Contact

Ready to receive.

Waiting for connection - 1:38

3. After successfully connecting to the remote device, the screen report Connected.
4. If two minutes passes before you connect, tap **Wait Again**.
5. File sharing is enabled until you end it by tapping **Cancel**.

Using the Dialer

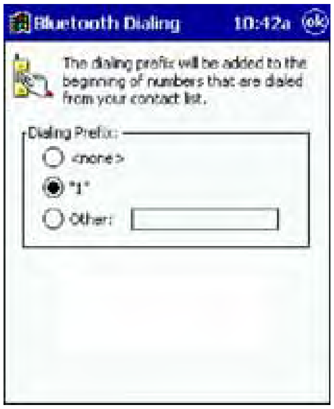
This section explains how to assign a dialing prefix and use the Dialer to dial a number directly from your Contacts list. The Dialer makes it quick and easy to perform dial-up networking.

Note: The Dialer has been verified to work with Nokia and Ericcson phones and is known not to work with the Motorola 270c, NTT Docomo Paldio 633S or Sony au C413S phone. Results may vary with other phones that are not listed as being supported by the Bluetooth system.

Assign a Dialing Prefix

If you have not already assigned a dialing prefix during the install process, you can do so by following these steps:

1. Go to **Start** > **Settings** > **System** tab. Tap on **Dialer**.
2. Select the appropriate Dialing Prefix, then tap **OK**.

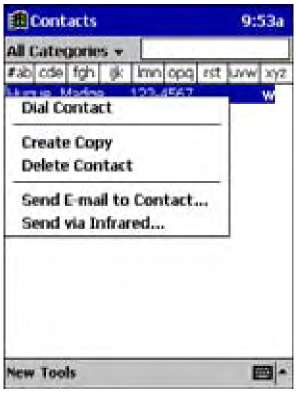


The dialing prefix will be added to the beginning of numbers that are dialed from your contact list.

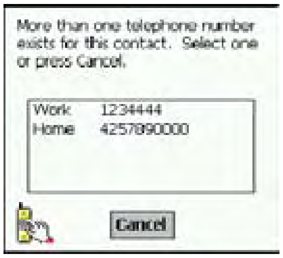
Dialing Prefix:
○ <none>
● "1"
○ Other:

Using the Dialer

1. To use the dialer, the mobile computer must already be connected to the Bluetooth phone. You can use the Get Connected! Wizard to do this. Also, the Bluetooth phone must be selected as your favorite.
2. Go to **Start** > **Contacts**.
3. Tap and hold your stylus on the contact you wish to dial to. In the pop-up menu, select **Dial Contact**. Alternatively, you can tap on **Tools** and select **Dial Contact**.



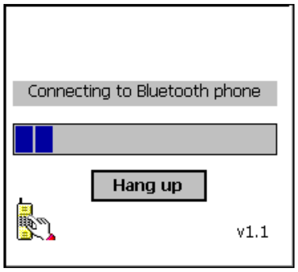
4. If you have multiple phone numbers for a contact, a screen appears listing them, including any dialing prefix you may have assigned. Select the phone number you wish to dial.



More than one telephone number exists for this contact. Select one or press Cancel.

Work	1234444
Home	4257890000

5. Your mobile computer connects to your phone and begins dialing.



Connecting to Bluetooth phone

The Dialer can dial a phone number containing any of the following non-numeric characters:

*   #   +   .   /   !   @   -   \   space   A   B   C   D   T   P   W

The following string can also be included in a phone number: (',')

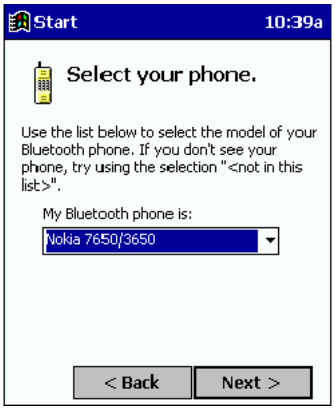
The Dialer cannot dial a phone number containing non-numeric characters other than those listed above. HHP recommends that you follow the standard Microsoft Outlook format for phone numbers.

Get Connected Wizard

The Get Connected! Wizard guides you through a one-time setup process that prepares the mobile computer and phone for Bluetooth connections. The wizard varies depending on what phone you want to connect to.

Ericcson, Nokia 6210, NTT DoCoMo, Sony Phones

1. Tap on the **Bluetooth** task tray icon. In the pop-up menu, select **Get Connected!**
2. Follow the Bluetooth “Get Connected!” Wizard. In the second screen, use the drop-down list to select your Bluetooth phone. The wizard provides tailored instructions based on your selection.



Select your phone.

Use the list below to select the model of your Bluetooth phone. If you don't see your phone, try using the selection "<not in this list>".

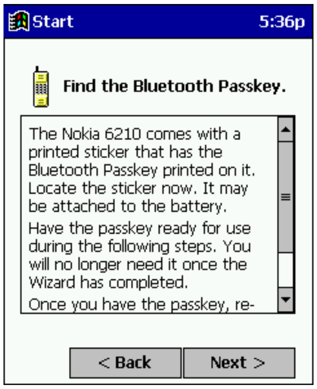
My Bluetooth phone is: Nokia 7650/3650

3. Follow the next screen(s) to prepare your specific phone for Bluetooth connections. You may need to do 1, 2 or all of the following steps:

(a) Naming your Bluetooth phone

(b) Setting your Bluetooth phone in Discoverable mode

(c) Preparing your Bluetooth passkey.



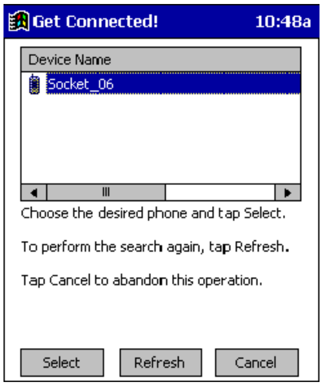
Find the Bluetooth Passkey.

The Nokia 6210 comes with a printed sticker that has the Bluetooth Passkey printed on it. Locate the sticker now. It may be attached to the battery.

Have the passkey ready for use during the following steps. You will no longer need it once the Wizard has completed.

Once you have the passkey, re-

4. When the search is complete, a list of the discovered Bluetooth phones appears. Choose the phone you wish to connect to, and tap **Select**. A service discovery phase begins, about 5-10 seconds.



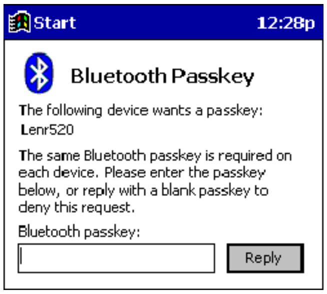
Choose the desired phone and tap Select.

To perform the search again, tap Refresh.

Tap Cancel to abandon this operation.

5. As prompted in the next screen, prepare your phone for bonding. For instructions on setting your phone to “Bondable” or “Pairable” mode, refer to your phone manual. Have your passkey ready, then tap **Next>**.

6. In the next screen, enter the passkey. Tap **Reply**.



Bluetooth Passkey

The following device wants a passkey:
Lenr520

The same Bluetooth passkey is required on each device. Please enter the passkey below, or reply with a blank passkey to deny this request.

Bluetooth passkey:

7. The mobile phone may then either automatically accept the passkey or ask you to enter one. If prompted for a passkey, use the same one you entered on the mobile computer.

Ericsson T68/T68i only: When the phone asks you if you want to bond, select 2: Add to paired devices. Do not tap ACCEPT.

8. Tap **Finish**. After successfully connecting, the phone appears in the Bluetooth Devices folder. On the Today screen, the Bluetooth icon blinks. You do not need to run the Get Connected! Wizard again unless you plan to switch between different phones.

Note: You may also switch between different phones by assigning a new “favorite phone” in the Bluetooth Devices folder.

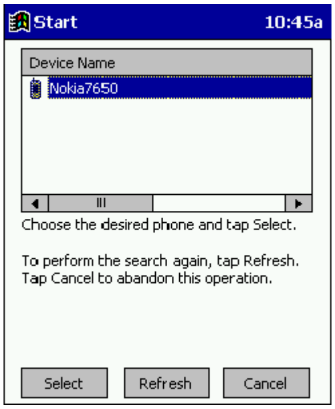
Motorola Timeport 270C, Nokia 3650/6310/7650/8910/8910i

1. Tap on the **Bluetooth** task tray icon. In the pop-up menu, select **Get Connected!**
2. Follow the Bluetooth “Get Connected!” Wizard. In the second screen, use the drop-down list to select your Bluetooth phone. The wizard provides tailored instructions for your phone.

Note: The screens below are for the Nokia 7650.

3. As directed on the next two screens, assign the phone a unique name, set the phone to Discoverable mode, and tap **Next**.

4. The mobile computer searches for the phone. When the search is over, a list of the discovered Bluetooth phones appears.



Device Name

Nokia7650

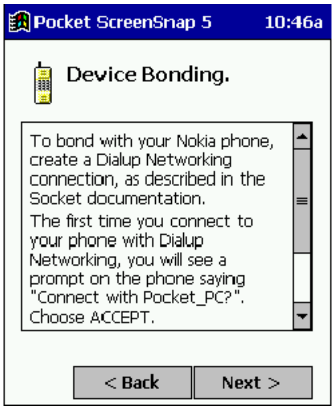
Choose the desired phone and tap Select.

To perform the search again, tap Refresh.
Tap Cancel to abandon this operation.

5. Choose the phone you want to connect to, and tap **Select**. A service discovery phase begins, about 5-10 seconds.

6. The next two screens describe procedures you complete outside of the wizard. Read through each screen but do not complete the described procedures until you exit the wizard.

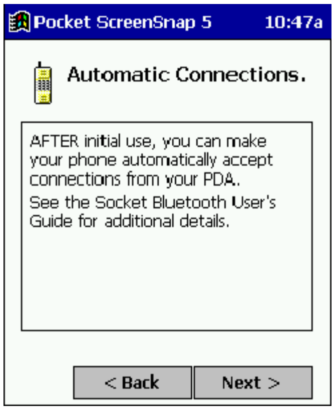
Bonding with your phone - This must be completed to establish the Bluetooth connection and involves dial-up networking.



Device Bonding.

To bond with your Nokia phone, create a Dialup Networking connection, as described in the Socket documentation.
The first time you connect to your phone with Dialup Networking, you will see a prompt on the phone saying "Connect with Pocket_PC?". Choose ACCEPT.

Automatic Connections - This procedure is optional but makes future Bluetooth connections more convenient.



Automatic Connections.

AFTER initial use, you can make your phone automatically accept connections from your PDA.
See the Socket Bluetooth User's Guide for additional details.

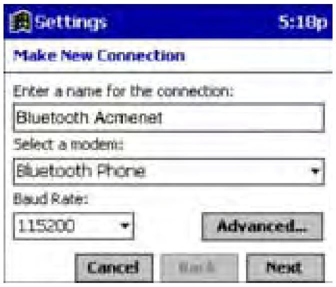
7. Continue to the last screen of the wizard and tap **Finish**. Now proceed to STEP 6 to complete the bonding process and, if desired, set up automatic connections.

Dial Up to Your Network

Complete the following steps to create a new Bluetooth internet connection. Before setting up dial-up networking, prepare yourself with dial-up information and other necessary settings from your office network or ISP.

Note: For more information about modem connections, see Creating an External Modem Connection to an ISP on page 7-23.

1. Go to **Start** > **Settings** > **Connections** tab **> Connections**.
2. In the top field, select **Internet Settings** and tap **Modify**. Then, tap **New**.



Settings 5:18p

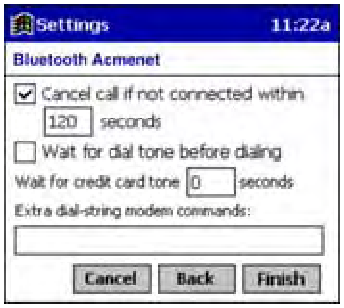
Make New Connection

Enter a name for the connection: Bluetooth Acmenet

Select a modem: Bluetooth Phone

Baud Rate: 115200

3. **Enter a name for the connection**. Remember what you name the connection. In the future, you will need to select it to start the connection.
   For the modem, select **Bluetooth Phone**.
   For the Baud Rate, select **115200**.
   If you want to configure Port Settings, TCP/IP, or Name Server settings, navigate to the setting and tap **Advanced**.
4. Tap **Next**.
5. In the Phone number field, enter the dial-up number. Tap **Next**.
6. Uncheck **Wait for dial tone before dialing**. Tap **Finish**.



Settings 11:22a

Bluetooth Acmenet

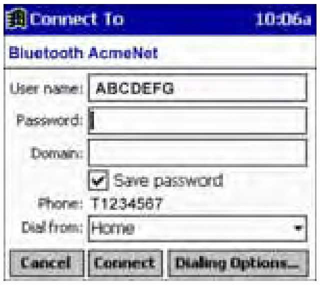
☑ Cancel call if not connected within 120 seconds

☐ Wait for dial tone before dialing

Wait for credit card tone 0 seconds

Extra dial-string modem commands:

7. Now you are ready to start the connection. In the Connections screen, under Internet Settings, tap **Connect**. In Network Log On, verify the dialing settings. Tap **OK**.



Connect To 10:06a

Bluetooth AcmeNet

User name: ABCDEFG

Password:

Domain:

☑ Save password

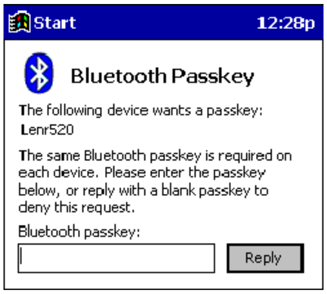
Phone: T1234567

Dial from: Home

ONLY FOR MOTOROLA TIMEPORT 270C OR NOKIA 3650/6310/7650/8910/8910i:

a) After you tap **Connect** for the first time, the phone displays a message asking if you want to bond. On Motorola, enter GRANT; on Nokia, enter ACCEPT.

b) Make up a 4-16 digit passkey, enter it on the phone, then enter it on the terminal.



The following device wants a passkey:
Lenr520
The same Bluetooth passkey is required on each device. Please enter the passkey below, or reply with a blank passkey to deny this request.
Bluetooth passkey:

Note: The Bluetooth icon on the Today screen blinks to indicate a connection.

c) After successfully bonding, you can set up the phone to automatically connect to your Dolphin 7900 without a passkey.

Automatic Connections for Motorola Timeport 270C:

- On the phone, press MENU.
- Scroll to Settings, then press SELECT.
- Scroll to Connection, then press ON.
- On Bluetooth Link, press SELECT.
- Scroll to Devices, then press SELECT.
- Choose your mobile computer, then press EDIT.
- Scroll to Access:Ask, then press CHANGE.
- Scroll to Automatic, then press SELECT. Press DONE.

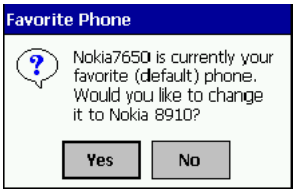
Automatic Connections for Nokia 3650/7650:

- On the phone, press MENU.
- Scroll to Connectivity, then press OPTIONS.
- The Open option should be highlighted. Press SELECT.
- The Bluetooth option should be highlighted. Press OPTIONS.
- The Open option should be highlighted. Press SELECT.
- Scroll to the right tab to access the Paired devices list. Highlight your mobile computer, then press OPTIONS.
- Scroll to Set as authorized, then press SELECT.
- In the confirmation screen, press YES.

Automatic Connections for Nokia 6310/8910/8910i:

- On the phone, press MENU.
- Scroll to 10 Bluetooth, then press SELECT.
- Scroll to 4 View Paired Devices, then press SELECT.
- Highlight the Dolphin 7900, then press OPTIONS.
- Scroll to 3 Request Connection Authorization, then press NO.

To use a different Bluetooth phone for dial-up networking, you can use the same connection setup, but you must make the new phone your favorite. Just run the Get Connected! Wizard again, select the new phone, and make it your new Favorite when prompted.



Nokia7650 is currently your favorite (default) phone. Would you like to change it to Nokia 8910?