HandHeld PRODUCTS

Image Kiosk 8560

with Microsoft® Windows® CE

powered by Adaptus™ imaging technology 5.0

User's Guide- Preliminary CP4 Draft

Disclaimer

Hand Held Products, Inc. (“Hand Held Products”) 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 Hand Held Products to determine whether any such changes have been made. The information in this publication does not represent a commitment on the part of Hand Held Products.

Hand Held Products 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.handheld.com

Trademarks

Microsoft, Windows, Windows CE, 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.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the property of their respective owners.

Table of Contents

Chapter 1 - Agency Information

Chapter 2 - Getting Started

Chapter 3 - Hardware Overview

Chapter 4 - Communication

Chapter 5 - IK8560C—Wireless LAN with 802.11b

Chapter 6 - Imaging

Chapter 7 - Mounting

Chapter 8 - Customer Support

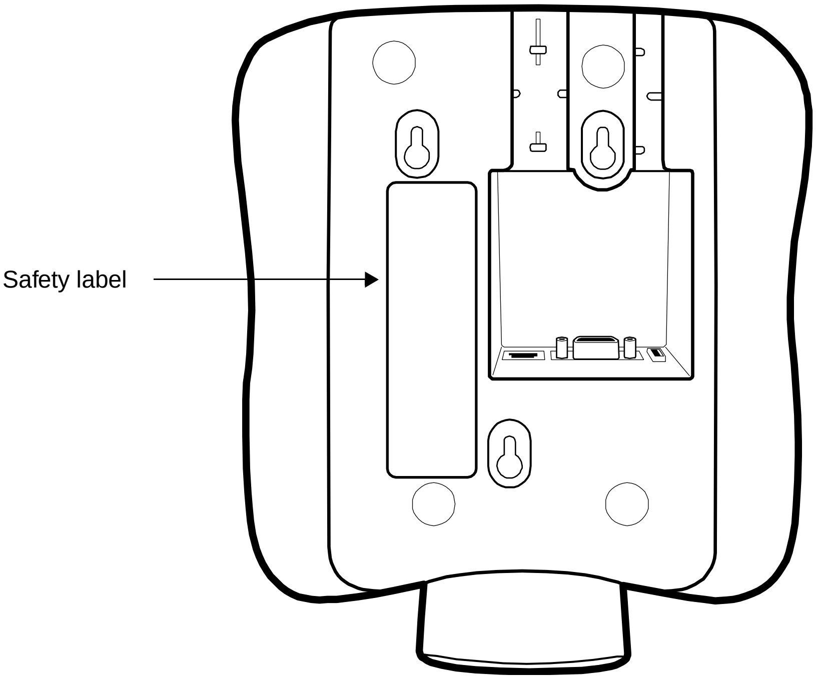
1

Agency Information

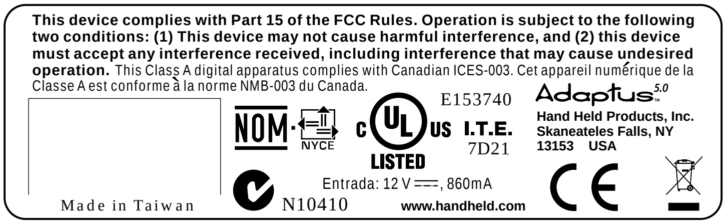
Required Safety Labels

Image Kiosk 8560 (IK8560) devices 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 IK8560.

Location



Safety Label, non-RF



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, and (2) this device must accept any interference received, including interference that may cause undesired operation. This Class A digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la Classe A est conforme à la norme NMB-003 du Canada.

NOM · NYCE

c UL US LISTED E153740 I.T.E. 7D21

Adaptus 5.0

Hand Held Products, Inc.
Skaneateles Falls, NY
13153 USA

Made in Taiwan

N10410

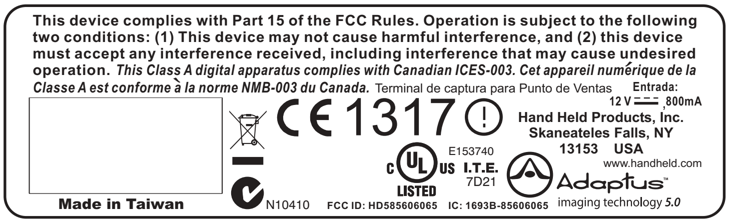
Entrada: 12 V ⎓, 860mA

www.handheld.com

CE

Safety Label, 802.11b Radio

IK8560 RF devices 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).



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, and (2) this device must accept any interference received, including interference that may cause undesired operation. ***This Class A digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la Classe A est conforme à la norme NMB-003 du Canada.*** Terminal de captura para Punto de Ventas

Entrada:
12 V ⎓ ,800mA

CE 1317 ⓘ

Hand Held Products, Inc.
Skaneateles Falls, NY
13153 USA
www.handheld.com

c UL US LISTED E153740 I.T.E. 7D21

Adaptus™ imaging technology *5.0*

Made in Taiwan

N10410 **FCC ID: HD585606065** **IC: 1693B-85606065**

Regulatory and Safety Approvals for all IK8560 Devices

Parameter	Specification
U.S.A.	FCC Part 15, Class A
Canada	ICES-003
European Community	EN 55022 (CISPR 22) Class A; 1998 +A1:2000; +A2:2003 EN60950 EN60825-1 EN55024:1998; +A1:2000; +A2:2003

CE 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

Hand Held Products, Inc. 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.

FCC Compliance

IK8560 devices meet or exceed all applicable standards and have been manufactured to the highest level of quality.

IK8560 Batch Device

IK8560 Batch devices comply with part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IK8560 RF Device With an 802.11b Radio

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio frequencies. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

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, use only the accessories specified by the manufacturer.**

Canadian Compliance for IK8560 RF Devices With an 802.11b Radio

This Class A digital apparatus complies with Canadian ICES-003. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (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

Parameter	Specification
RF Approvals	
U.S.A.	FCC Part 15-247
Canada	RSS 210, RSS GEN
Europe	EN300328-1, V.1.6.1:2004-11 EN301489-1, V.1.6.1:2005-09 EN301489-17, V.1.2.1:2002-08

This product is marked with CE 1317 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

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 IK8560 is 0.3V/m according to Subpart B of Part 1 of the FCC rules. Therefore, the IK8560 RF has no effect on medical devices that meet the IEC specification.

Microwaves

The radio in the IK8560 RF device operates on the same frequency band as a microwave oven. Therefore, if you use a microwave within range of the IK8560 RF device you may notice performance degradation in your wireless network. However, both your microwave and your wireless network will continue to function.

The IK8560 batch device does not contain a radio, and therefore, is not affected by microwave ovens.

Care and Cleaning

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

For European Community Users

Hand Held Products complies with Directive 2002/69/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 January 2003 on waste electrical and electronic equipment (WEEE).

Waste Electrical and Electronic Equipment Information

This product has required the extraction and use of natural resources for its production. It may contain hazardous substances that could impact health and the environment, if not properly disposed.

In order to avoid the dissemination of those substances in our environment and to diminish the pressure on the natural resources, we encourage you to use the appropriate take-back systems for product disposal. Those systems will reuse or recycle most of the materials of the product you are disposing in a sound way.

The crossed out wheeled bin symbol informs you that the product should not be disposed of along with municipal waste and invites you to use the appropriate separate take-back systems for product disposal.

If you need more information on the collection, reuse, and recycling systems, please contact your local or regional waste administration.

You may also contact your supplier for more information on the environmental performances of this product.

2

Getting Started

IK8560 Features

The IK8560 comes in two standard versions: the IK8560C with an on-board 802.11b radio and the IK8560E with a wired ethernet connection. Here is a list of the standard features:

- Microsoft Windows CE 5.0 operating system
- Intel® XScale PXA 255 200MHz processor
- 5.7" 320X240 backlit color display
- Touch screen and protective overlay
- 64 MB SDRAM and 32 MB Flash ROM of on-board memory
- Support for RS-232, RS-485, USB, and powered USB interfaces
- Ethernet 10/100 Base-T communications port (IK8560E)
- 802.11b wireless radio (IK8560C)
- USB host communications port
- Adaptus Imaging Technology
- Beeper

Connect the Power and Communication Cables

The IK8560 has a number of power and communication cables. Use one to apply power to the device.

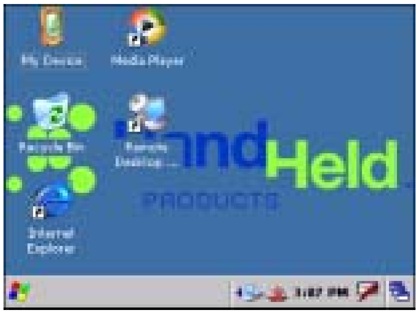
For more information, see Connecting the Power and Communication Cables on page 3-4.

Boot the IK8560

1. The IK8560 begins booting as soon as power is applied from the cable.
2. The splash screen appears as the system cold boots (see Cold Boot on page 3-6). The software version numbers for both the bootloader and the kernel appear on the splash screen.
3. The device begins loading software; this is Autoinstall. A status bar appears for each program that loads. Do NOT interrupt Autoinstall!
4. Autoinstall completes and the splash screen appears again as the system warm boots (see Warm Boot on page 3-6).
5. When the warm boot is complete, you end on the Start screen.

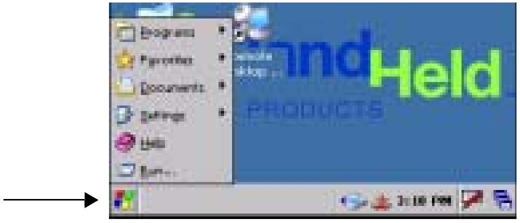
Start Screen

The Start screen is your Desktop for the IK8560. The boot process ends on this screen.

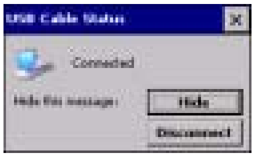
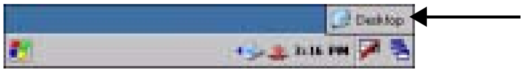


Task Tray

The task tray is located at the bottom of every application window and provides access to the Start menu.

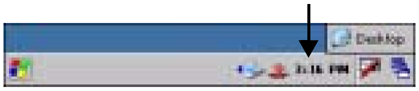


Task Tray Icons

Icon	Description
	Opens the Start menu.
	The communication cable is connected. Double-tapping this icon displays the cable type and connection status.  USB Cable Status Connected Hide this message: Hide Disconnect
	Wired ethernet cable is not connected.
	802.11b radio is not connected
	802.11b radio is connected.
	Displays the Soft Input Panel (SIP); see Using the Soft Input Panel (SIP) on page 2-3.
	Tapping this button enables you to return to the Desktop.  The pop-up menu that appears will also show two programs or windows currently open.

Setting the Time and Date

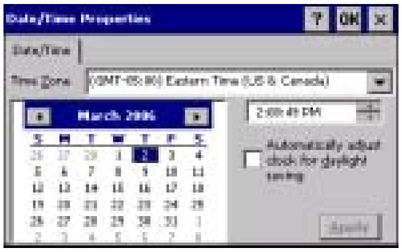
After the device boots up, set the time and date to set the system clock to real-time.



Double-tap the time on the taskbar

OR

Tap **Start** > **Control Panel** > **Date/Time**.

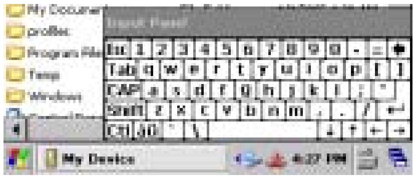

Date/Time Properties
? OK ×
Date/Time
Time Zone: (GMT-05:00) Eastern Time (US & Canada)
March 2006
2:08:49 PM
Automatically adjust clock for daylight saving
Apply

The date and time saved here sets the system clock. Any scheduled function runs off the system clock.

Using the Soft Input Panel (SIP)

The SIP is a soft keyboard that enters text into fields and screens. The SIP pops up automatically over certain screens that require text entry. You can also manually open the SIP when needed.

To open the SIP, tap the **Input Panel** icon in the task tray and select **Keyboard** on the pop-up menu.

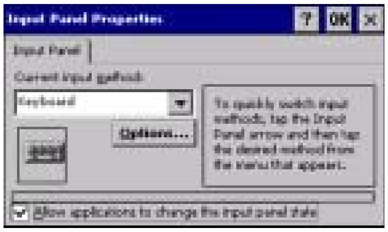


On the soft keyboard that displays, tap the character keys to enter them on the screen.

To close the SIP, tap the **Input Panel** icon again and select **Hide Input Panel**.

SIP Settings

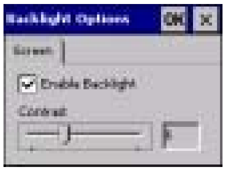
You can adjust SIP panel settings by tapping **Start** > **Settings** > **Control Panel** > **Input Panel**.


Input Panel Properties
? OK ×
Input Panel
Current input method:
Keyboard
Options...
To quickly switch input methods, tap the Input Panel arrow and then tap the desired method from the menu that appears.
Allow applications to change the input panel state

Allow applications to change the input panel state is selected by default and makes the SIP appear automatically in applications when text needs to be typed. If you de-select this option, you must manually tap the SIP button every time you want to use the SIP.

Adjusting the Backlight

Tap **Start** > **Settings** > **Control Panel** > **Display** > **Backlight** tab > **Advanced**. The Backlight Options window opens.



The backlight is on by default (and enabled after each re-boot).

To turn off the backlight, de-select the **Enable Backlight** option (not recommended except for test purposes). Because the screen goes completely dark, the best way to enable the backlight again is to power cycle, which re-boots the unit. While the screen is dark, the Enable Backlight option is still there but can't be seen to be selected accurately.

Adjusting the Contrast

On the Backlight Options window, use the **Contrast** slider to adjust the contrast.

Using Windows Explorer

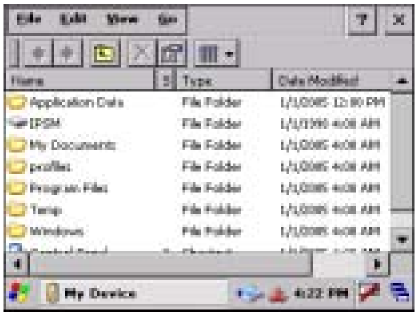
You can access Windows Explorer by

Double-tapping the **My Device** icon on the start screen My Device.

OR

Tapping **Start** > **Windows Explorer**.

Windows Explorer opens to the root folder level.



Name	S	Type	Date Modified
Application Data		File Folder	1/1/2005 12:00 PM
IPSM		File Folder	1/1/1990 4:08 AM
My Documents		File Folder	1/1/2005 4:08 AM
profiles		File Folder	1/1/2005 4:08 AM
Program Files		File Folder	1/1/2005 4:08 AM
Temp		File Folder	1/1/2005 4:08 AM
Windows		File Folder	1/1/2005 4:08 AM

Use Windows Explorer to find and move files.

Selecting Text

To edit or format typed text, select it by dragging your finger across the text. Tap and hold the selection, then use the commands on the pop-up menu to cut, copy, and paste the selected text.

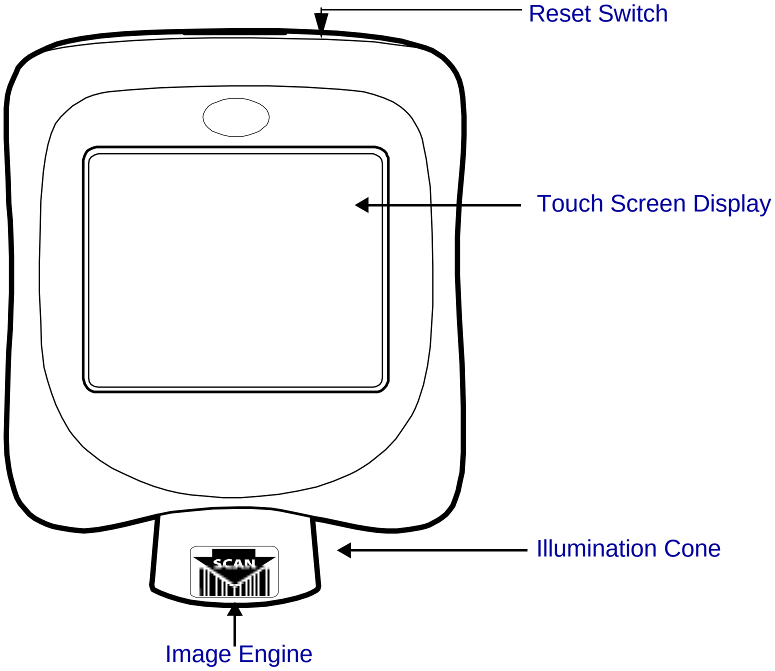
Selecting Programs

To launch a program, tap **Start** > **Programs** and select a program from the list.

3 Hardware Overview

Front Panel

This section describes features on the front panel of the IK8560 device.



Reset Switch

This switch performs a cold boot without removing power from the unit. For details, see Using the Reset Switch on page 3-6.

Touch Screen Display

The device features a 5.7" QVGA transmissive LCD color display that is backlit for maximum viewability, then covered with an industrial touch screen protector for maximum durability. The touch screen resolution is 903 x 1238 points per inch (PPI). For touch screen input, use your finger.

⚠ *Use of objects, such as paper clips, pencils, or ink pens on the touch screen can damage the input panel and will void the warranty.*

Screen Protectors—Hand Held Products requires 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 Hand Held Products (p/n 100000583). You can replace the touch screen protector; see Screen Protector Replacement on page 3-7.

Beeper

The internal beeper generates a tone for successful decoding.

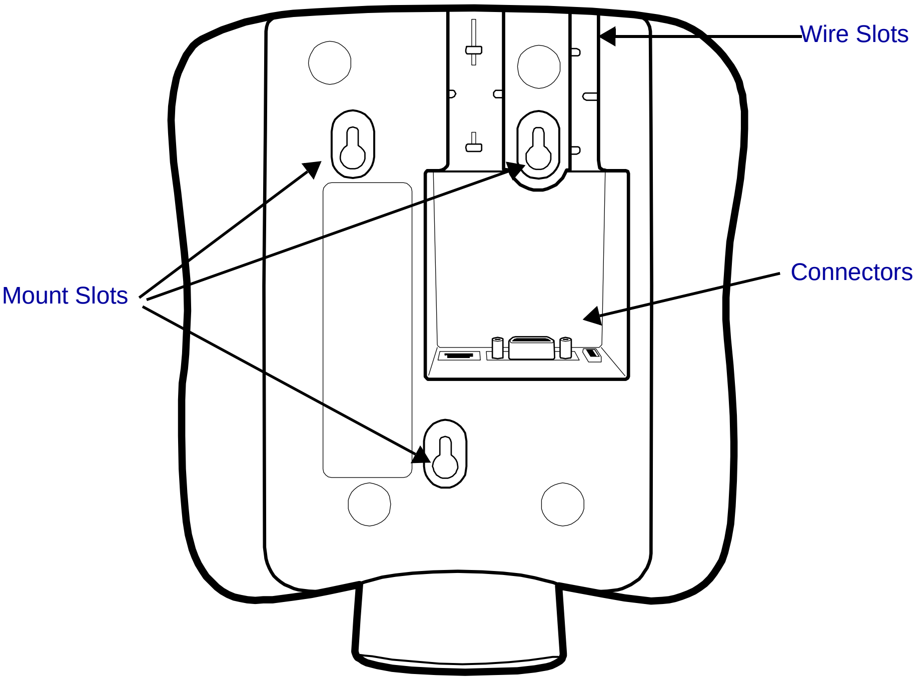
Illumination Cone

Projecting downward from the front panel, the image engine cone houses the image engine. Slide the bar code underneath this slot to scan a bar code or take an image. See Scanning a Bar Code on page 6-2.

Image Engine

The red illumination LEDs project out from the image engine at all times. For more information about imaging, see Imaging on page 6-1.

Back Panel



The back panel is designed for easy mounting, either to a wall or stand.

Wire Slots

These two slots are designed to hold the wires of the connecting cables.

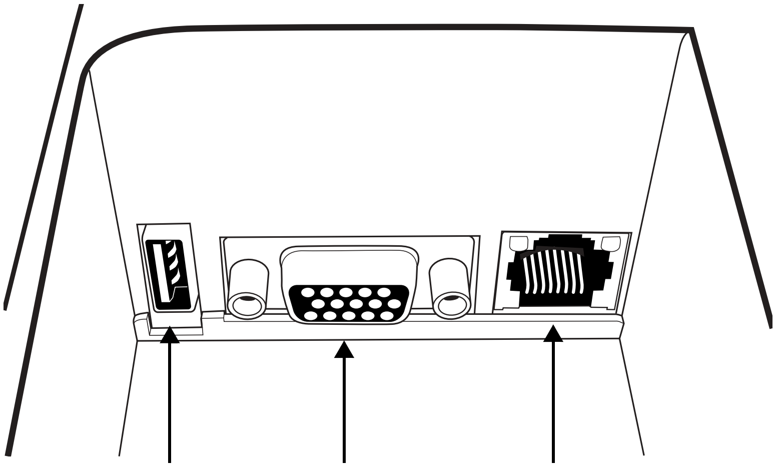
Connectors

There are three connectors in a slot inside the back panel; see Connectors on page 3-3.

Mount Slots

Use these slots to mount the IK8560 to a flat surface or bracket. For mounting specifications, see Mounting on page 7-1.

Connectors



USB Host Port

The USB Host port features a 5V DC power pass-through and can host supported USB client devices. Multiple USB devices can be accommodated by plugging a USB HUB into the USB Host port. This is a four-pin connector and supports USB 1.1 communication. USB 2.0 devices that are backwards compatible with USB 1.1 may be connected to this port but will operate at USB 1.1 speeds.

For more information, see USB Host Port on page 4-9.

DB15 Connector

This is a single 15-pin, D-style, high-density female connector. All power cables have a connector that matches this pin configuration. This connector powers the device (by receiving power from the cable) and communicates with a host workstation using ActiveSync (USB only).

For more information, see Microsoft ActiveSync on page 4-2.

RJ45 Jack

IK8560E—On the IK8560E unit, this is a 10/100 Base-T communications port that supports wired ethernet communications with a standard RJ45 ethernet cable. Cable must be purchased separately. You cannot power the device through the ethernet cable. For more information, see Wired Ethernet Communication—IK8560E on page 4-8.

IK8560C—On the IK8560C unit, this connector is not enabled.

Connecting the Power and Communication Cables

The IK8560 features a standard power cable that connects to a number of communication cables to suit your environment.

Standard Power Cable

The standard power cable powers the device and with an AC power adapter to convert the voltage from the power source to the voltage required by the device. The IK8560 device must be connected to external power to run.

Communication Cables

The IK8560 offers the following communication options:

- USB Cable (four feet)
- Standard RS-232 Cable (12 feet)
- RS-232 Pass-Through (Y cable)

Note: You can verify the status of the communication cable by the icon in the task tray; see Task Tray Icons on page 2-2.

USB Cable

The USB communication cable is four feet long and supports USB 1.1. You can connect USB 2.0 devices that are backwards compatible with USB 1.1 with this cable but data transfer will occur 1.1 speeds.

It features a single, 15-pin male connector that plugs into the DB15-pin female port on the back panel. The other end features a standard Type A USB (1.1 or higher) connector designed to fit standard USB ports.

Note: Make sure the power switch is turned off on the computer where you will be installing the IK8560.

1. Plug the 15-pin connector (HDB15) of the communication cable into the back of the IK8560.

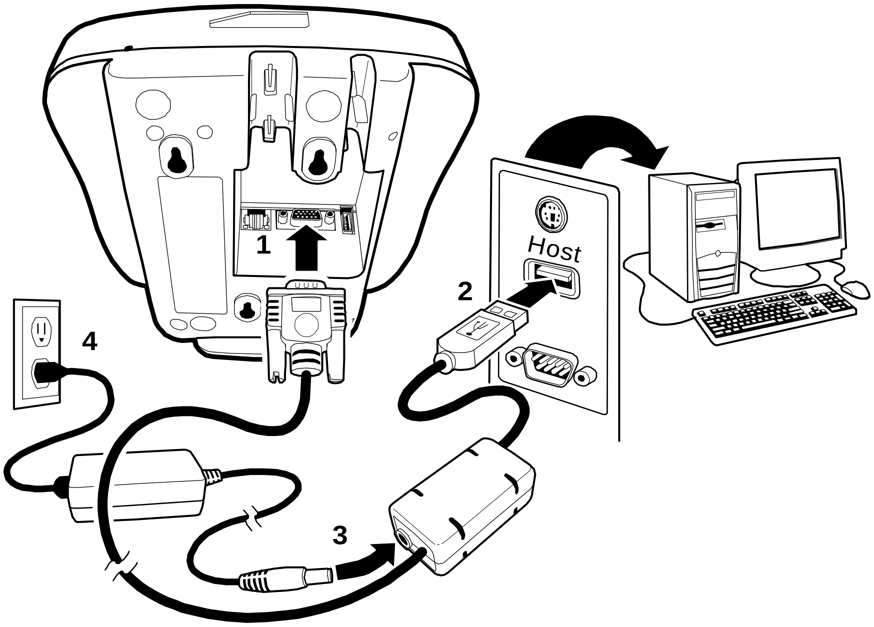
2. Plug the USB connector into the port on your host workstation.

3. Plug the power plug into the pod on the communication cable.

4. Plug the AC power supply into a power outlet.

Hardware installation is now complete. Your IK8560 powers on and auto-configures to USB.

When you power on the host workstation, you need to complete the Found New Hardware wizard and install the IK8560 driver to configure the workstation for ActiveSync communication; see Microsoft ActiveSync on page 4-2.



If you want to power the device without communicating, simply disconnect the USB connector from the host workstation.

Standard RS-232 Cable

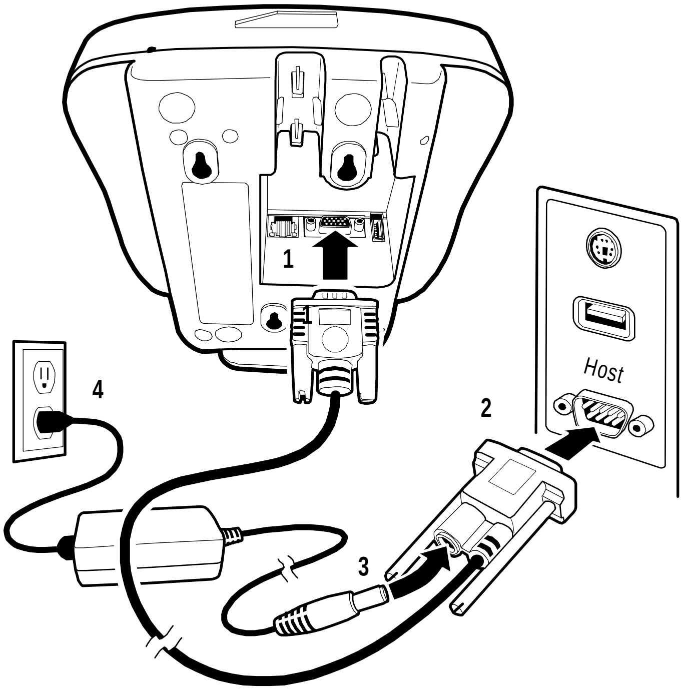
The standard RS-232 cable is 12 feet long and can connect to multiple devices but does not support ActiveSync communication.

Note: Make sure the power switch is turned off on the device where you will be installing the IK8560.

1. Plug the 15-pin connector (HDB15) of the serial cable into the underside of the IK8560.
2. Plug the 9-pin connector (DB9) of the serial cable into an available serial port on the device.
3. Plug the male connector of the AC power supply cable into the socket on the back of the DB9-pin serial cable connector, which is plugged into the back of your host device.
4. Plug the AC power supply into a power outlet.

Installation is now complete. Your IK8560 powers on and auto-configures to RS-232. You may now turn on your host device.

Note: If your computer has a 25-pin serial port, you will need to obtain a 25-pin to 9-pin adapter from your local computer store or other source.



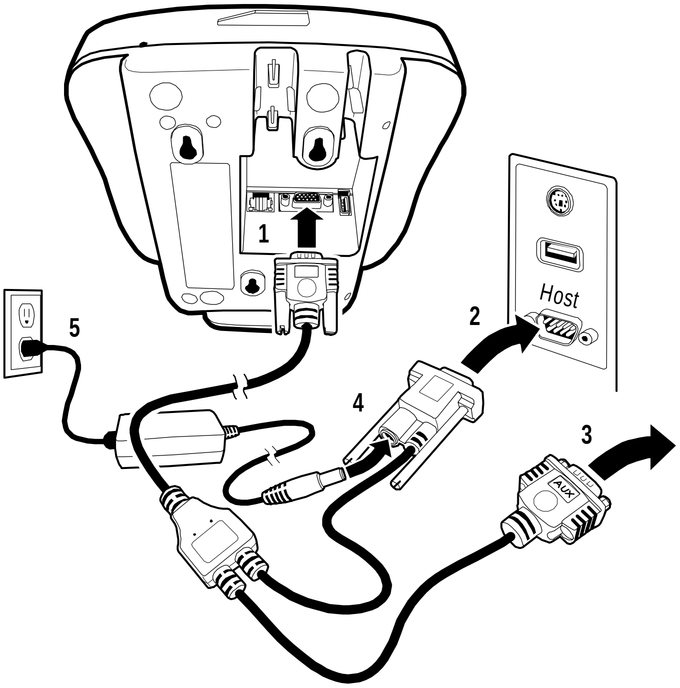
RS-232 Pass-Through Cable

The RS-232 pass-through cable uses a Y cable with AC power adapter.

Note: Make sure the power switch is turned off on the device where you will be installing the IK8560.

1. Plug the 15-pin connector (HDB15) of the serial cable into the underside of the IK8560.
2. Plug the Host DB9 connector into your host workstation.
3. Plug the Aux DB9 connector into the other RS-232 device.
4. Plug the male connector of the AC power adapter cable into the socket on the back of the DB9-pin serial cable connector, which is plugged into the back of your host device.
5. Plug the AC power supply into a power outlet.

Installation is now complete. Your IK8560 powers on and auto-configures to RS-232. You may now turn on your host device.



Rebooting the Device

There are two types of reboots: a warm boot and a cold boot.

Warm Boot

A warm boot reboots the device without erasing data and applications stored in RAM memory.
To launch a warm boot, tap **Start** > **Programs** > **Power Tools** > **Reboot** > **Warm Boot**.

Cold Boot

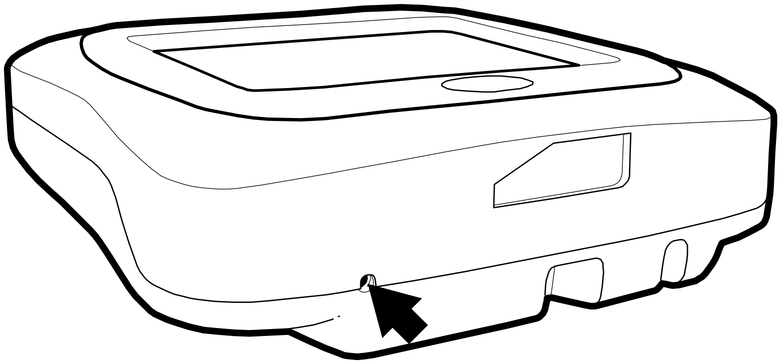
A cold boot reboots the device and re-installs the .cab files stored in the Autoinstall folder.
To launch a cold boot, you can

- Power cycle
- Perform a hard reset with the reset switch

⚠ *Cold boots erase data and applications stored in RAM memory.*

Using the Reset Switch

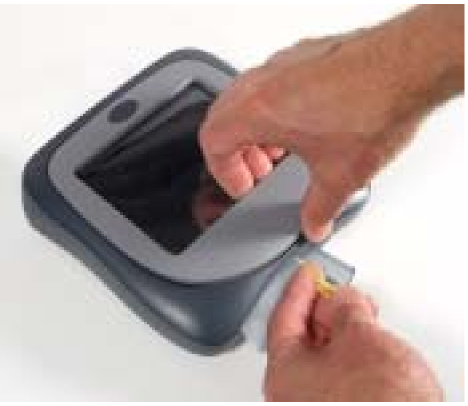
Power can be cycled (which performs a cold boot) by using the end of a straightened paper clip to push the reset switch on the top panel.



Screen Protector Replacement

Screen protectors can be purchased at any major computer retail store or directly from Hand Held Products (p/n 100000583).

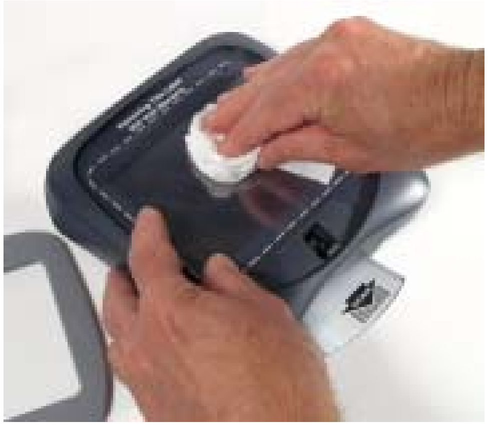
1. To remove the old screen protector frame, insert a straightened paper clip into the small hole in the front of the IK8560. This releases the protector frame which can now be lifted off.



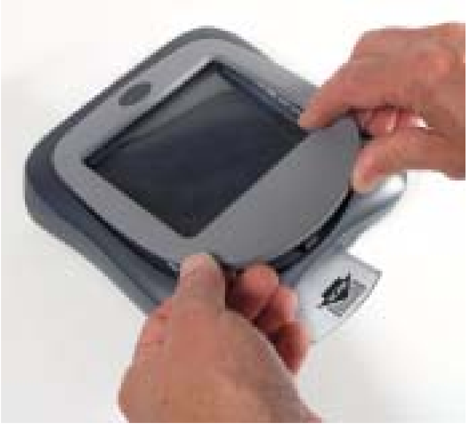
2. Clean any smudges or dirt from the IK8560 touch screen using glass cleaner or water. Wipe the surface dry.
3. Remove the protective film from the back of the new screen protector.

4. Line up the holes in the protector with the pins on the IK8560 screen.

5. Use a tissue or soft cloth to wipe the front of the screen protector. (This makes the protector lie flat.)



6. Place the protector frame back in place and press down until it snaps shut.



Maintenance

To clean your IK8560, use a soft cotton cloth lightly dampened with isopropyl alcohol. This removes any ink, fingerprint smudges, or dirt.

IK8560 Technical Specifications

Display Window	
Window	Resistive, transparent, pressure-sensitive touch screen
LCD Size	4.5 x 3.3 in. (11.3 x 8.4 cm) (Active area)
LCD Resolution	320 x 240 dot, 16-bit color
Touch Pad Resolution	903 x 1238 ppi
Communications	
RS-232	4800 to 115.2 Kbps
RS-232 Pass-Through	Using Aux. Y cable with AC power adapter
PC USB	AC power adapter required
USB Hub Host	5V DC power pass-through, support for USB 1.1 for up to 10 devices
Ethernet 10/100 BaseT	Optional port. Cable not supplied.
Radio Frequency	802.11b, optional (AC power adapter and power supply required; not included)
Memory	
Flash	32 MB non-volatile synchronous Flash standard
SDRAM	64MB
Dimensions (reference)	
Width	7.3 in. (18.5 cm)
Depth	7.6 in. (19.2 cm)
Height	3.2 in (8.03 cm)
Weight	2 lb. (.9 kg)
Power Requirements	
Current Draw	IK8560E (non-RF): 800mA @ 12V DC IK8560C (RF): 860mA @ 12V DC
Source	120V AC adapter or powered host terminal port
System Architecture	
Processor	Intel XScale PXA255 200 Mhz
Development Environment	Supports Visual Studio 2005 for C++, C#, and VB.net development

IK8560 Technical Specifications

Operating Platform	Microsoft Windows CE 5.0
Third Party Software	Hand Held Products Mobile Systems Manager
Graphics Supported	BMP, CGM, DIB, EPS, MF, PCL, PCX, PLS, JPG, and TIF
RF Security	WEP (64 and 128 bit), EAP, WPA
Approvals and Certifications	
Agency Conformance	FCC Class A, CE (LVD), UL 1950, CSA 22.2

4

Communication

Communication Options

There are a number of communications options.

Microsoft ActiveSync

The USB communication cable supports Microsoft ActiveSync communication. For more information, see Microsoft ActiveSync on page 4-2.

Wired Ethernet–IK8560E

IK8560E devices contain an ethernet port on the back panel that connects the device to an ethernet network via standard RJ45 cable. For information, see Wired Ethernet Communication—IK8560E on page 4-8.

USB Host Port

The USB host port on the back panel enables you to configure the IK8560 as a USB host connected to other USB devices. For more information, see USB Host Port on page 4-9.

802.11b Radio–IK8560C

The IK8560C contains an on-board 802.11b radio that establishes the device on a wireless network.
For information, see IK8560C—Wireless LAN with 802.11b on page 5-1.

Installing Additional Software

You can install additional programs on the IK8560 through most of the communication options. However, the following requirements must be met:

- The program must be created specifically for a Windows CE device and have an *.exe, *.cab, or *.dll extension.
- The device must have enough memory to store the program. To check memory allocation and usage, tap **Start** > **Settings** > **Control Panel** > **System** > **Memory** tab.

Verify that the program and version of the program are designed for Windows CE 5.0 and the Intel processor. Check both by tapping Start > Settings > Control Panel > System > General tab.

- See Adding Programs Using ActiveSync on page 4-6.
- See Adding Programs from a Network on page 4-8.

Microsoft ActiveSync

Microsoft ActiveSync connects the device to a host workstation, which enables you to

- Transfer files,
- Install additional programs, and
- Synchronize information between the workstation and the device.

Requirements

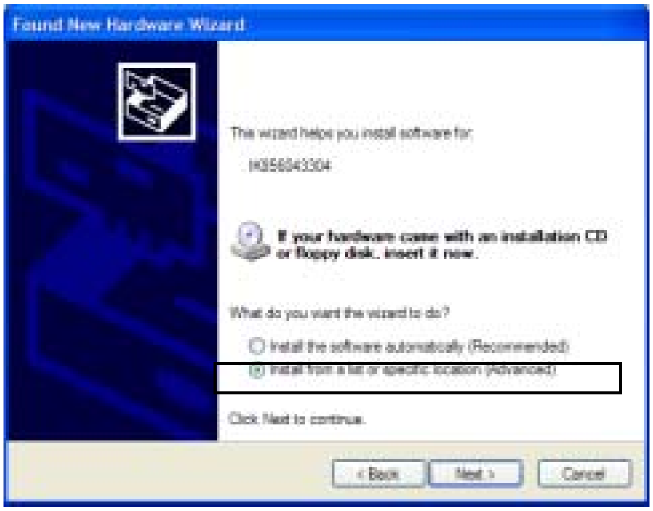
Using ActiveSync with the IK8560 device requires the following:

1. A USB communication cable connecting the host workstation and the IK8560 device; see USB Cable on page 3-4.
2. The **IK8560.inf** file installed on the hard drive of the host workstation.
3. ActiveSync version 4.1 or higher installed on both the host workstation and the IK8560 device.
   IK8560 devices ship with ActiveSync already installed. If ActiveSync is not already installed on the host workstation, you can download the latest version of ActiveSync from Microsoft's web site and run the install wizard.

Installing the .INF File on the Host Workstation

To establish an ActiveSync connection, you must install the **IK8560.inf** file on the host workstation. Once this file is installed, you will be able to use ActiveSync on the host workstation. You must repeat this process on each workstation where you want to use an ActiveSync connection to the IK8560.

1. When the device is connected to the host workstation via USB cable and both the device and the host workstation are powered on, the Found New Hardware Wizard opens on the workstation.
2. Select **Install from a list or specific location (Advanced)**.



Found New Hardware Wizard

This wizard helps you install software for:

IK856043304

If your hardware came with an installation CD or floppy disk, insert it now.

What do you want the wizard to do?

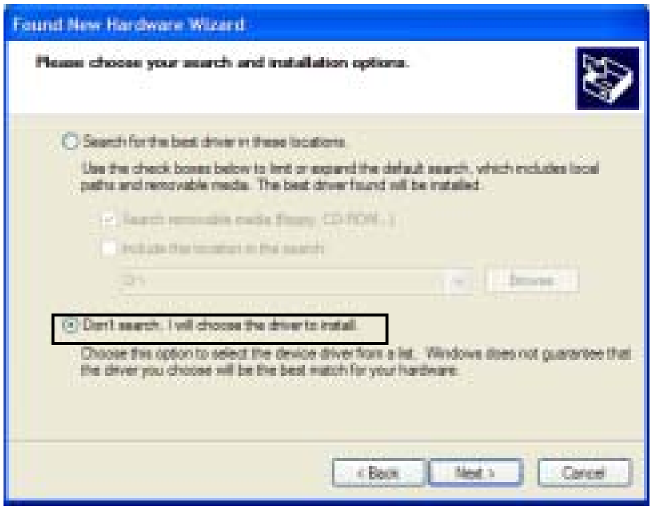
○ Install the software automatically (Recommended)

● Install from a list or specific location (Advanced)

Click Next to continue.

3. Click **Next**.

4. Select **Don’t Search. I will choose the driver to install**.



Found New Hardware Wizard

Please choose your search and installation options.

○ Search for the best driver in these locations.

Use the check boxes below to limit or expand the default search, which includes local paths and removable media. The best driver found will be installed.

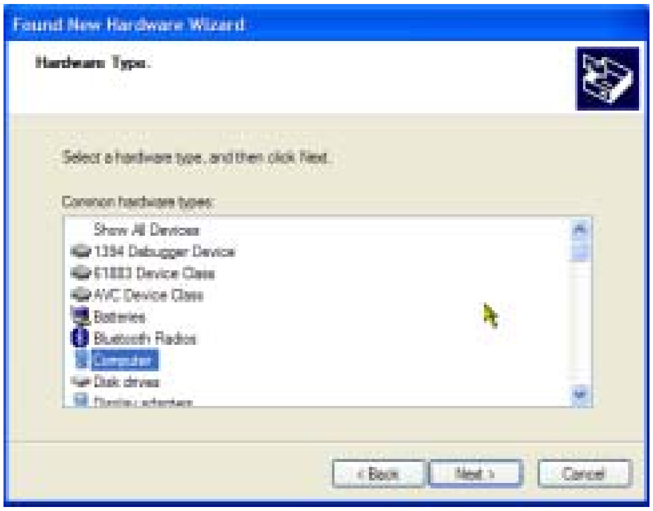
☑ Search removable media (floppy, CD-ROM...)

□ Include this location in the search:

● Don't search. I will choose the driver to install.

Choose this option to select the device driver from a list. Windows does not guarantee that the driver you choose will be the best match for your hardware.

5. Click **Next** and select **Computer** as the hardware type.



Found New Hardware Wizard

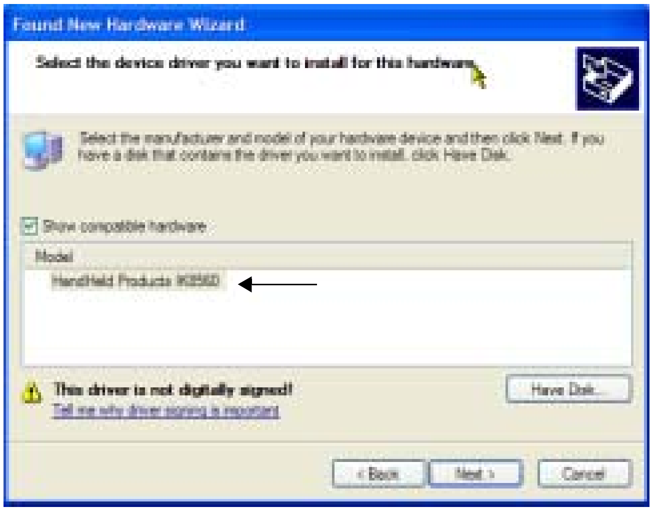
Hardware Type.

Select a hardware type, and then click Next.

Common hardware types:

6. Click **Next**. When the wizard tells you it can’t find drivers for the device, click **Have Disk**.

7. Navigate to where the **wceusbsh.inf** file is stored on the workstation and select it. The host workstation reads the file as “HandHeld Products TT8560.”



Found New Hardware Wizard

Select the device driver you want to install for this hardware.

Select the manufacturer and model of your hardware device and then click Next. If you have a disk that contains the driver you want to install, click Have Disk.

☑ Show compatible hardware

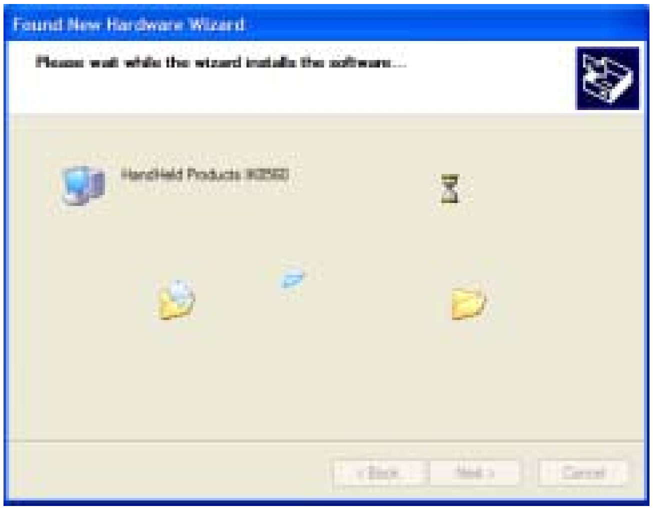
Model

HandHeld Products IK8560

This driver is not digitally signed!

Tell me why driver signing is important

8. Click **Next**. The hardware begins installing.



Found New Hardware Wizard

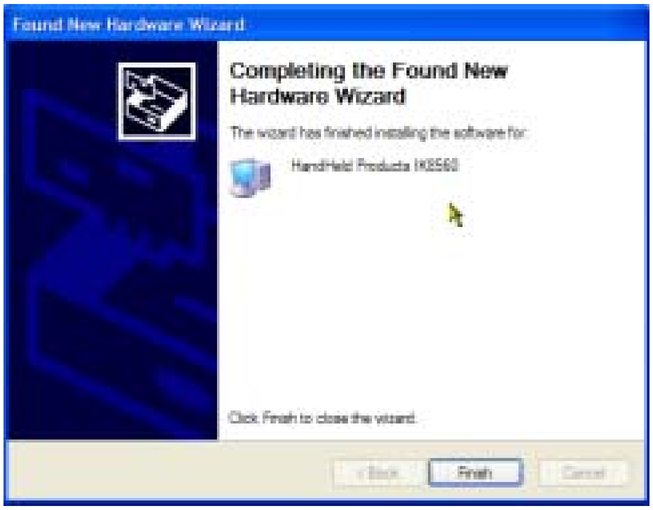
Please wait while the wizard installs the software...

HandHeld Products IK8560

9. You will see a brief flash on the IK8560 screen, then the ActiveSync Wizard appears on the workstation.

10. Complete the ActiveSync Setup Wizard. ActiveSync will auto-configure to USB communication.

11. The Found New Hardware Wizard notifies you that setup is complete.



Found New Hardware Wizard

Completing the Found New Hardware Wizard

The wizard has finished installing the software for:

HandHeld Products IK8560

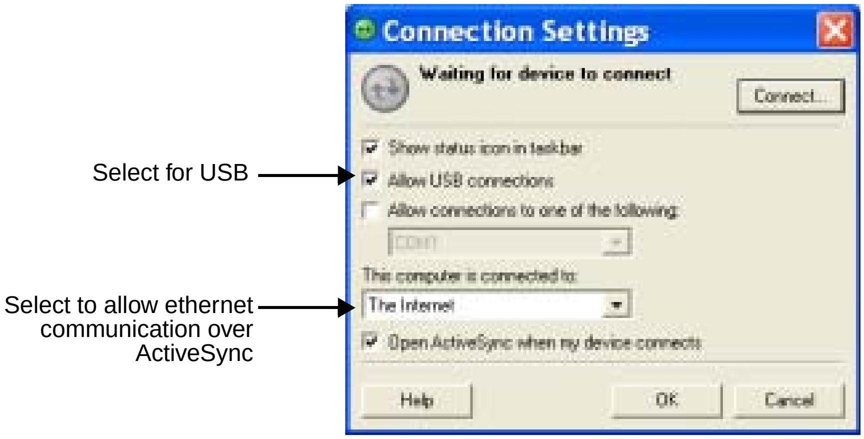
Click Finish to close the wizard.

12. Click **Finish** and you are now ready to use the ActiveSync connection.

Note: You can find more information about ActiveSync in the ActiveSync Help on your workstation. In ActiveSync, click Help > Microsoft ActiveSync Help.

Setting Up the Host Workstation

Verify that ActiveSync on the workstation has selected the appropriate communication type by clicking **File** > **Connection Settings**.



Connection Settings

Waiting for device to connect

☑ Show status icon in taskbar

☑ Allow USB connections

□ Allow connections to one of the following:

COM1

This computer is connected to:

The Internet

☑ Open ActiveSync when my device connects

Verify the communication type:

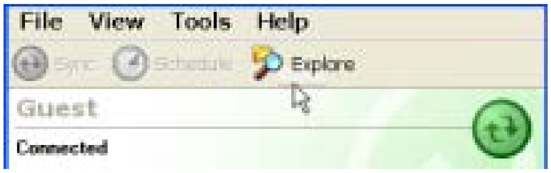
- For USB, select **Allow USB connections**. Do **not** check the serial cable box below it!
- To have ActiveSync work over the ethernet, in the **This computer is connected to** drop-down list, select **The Internet**.

Tap **OK** to save changes.

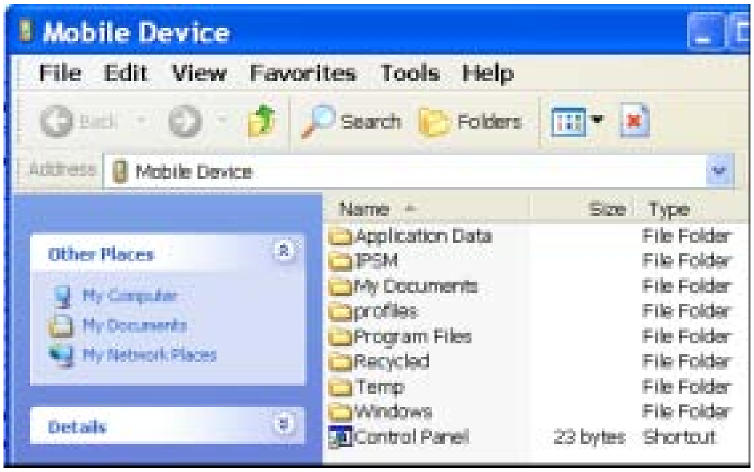
Exploring the Device from the Host Workstation

Use the Explore feature of ActiveSync to transfer files between the host workstation and the device.

When the device and host workstation are connected, open the main ActiveSync window, and click **Explore**.



The Mobile Device folder opens in Windows Explorer.



Name	Size	Type
Application Data		File Folder
IPSM		File Folder
My Documents		File Folder
profiles		File Folder
Program Files		File Folder
Recycled		File Folder
Temp		File Folder
Windows		File Folder
Control Panel	23 bytes	Shortcut

The device 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 Using ActiveSync

When selecting programs, verify that the version of the program is designed for Windows CE 5.0 and the Intel processor. Check both by tapping Start > Settings > Control Panel > System > General tab.

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

1. Download the program to the host workstation from either a network or CD-ROM. 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, Readme files, or documentation that comes with the program. Many programs provide special installation instructions.
3. Connect the device to the workstation using a Hand Held Products communication cable.

If the File is an Installer:

An installer program is one that installs to the workstation and the device simultaneously; one process installs to both devices.

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

If the File is Not an Installer:

Some programs cannot be installed on workstations. In these cases, the appropriate files must be stored on the host workstation, transferred to the device via ActiveSync, and installed on the device. You will know that the program cannot be installed on the workstation 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 Readme file or documentation, open **ActiveSync** and click **Explore**.*
2. Copy the program file or files to the **Program Files** folder on the device.

If you want the program to be part of the Autoinstall that occurs after every cold boot, place the program file in the **Autoinstall** folder (\\IPSM\AutoInstall).

3. Depending on the program, you may need to open **File Explorer** on the device, 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 cold boot and the program will install as part of the Autoinstall process. Remember! A cold boot erases RAM data and applications.

4. After installation on the device is complete, tap **Start** > **Programs** and the program appear on the menu. Tap it to open the program.

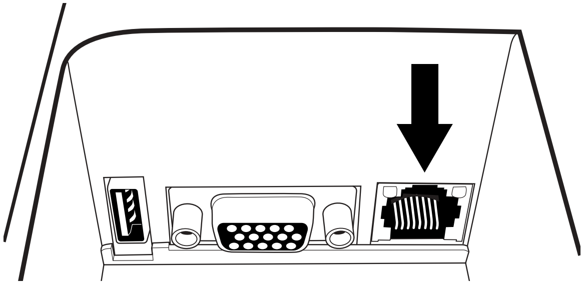
Synchronizing

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 workstation and your device.

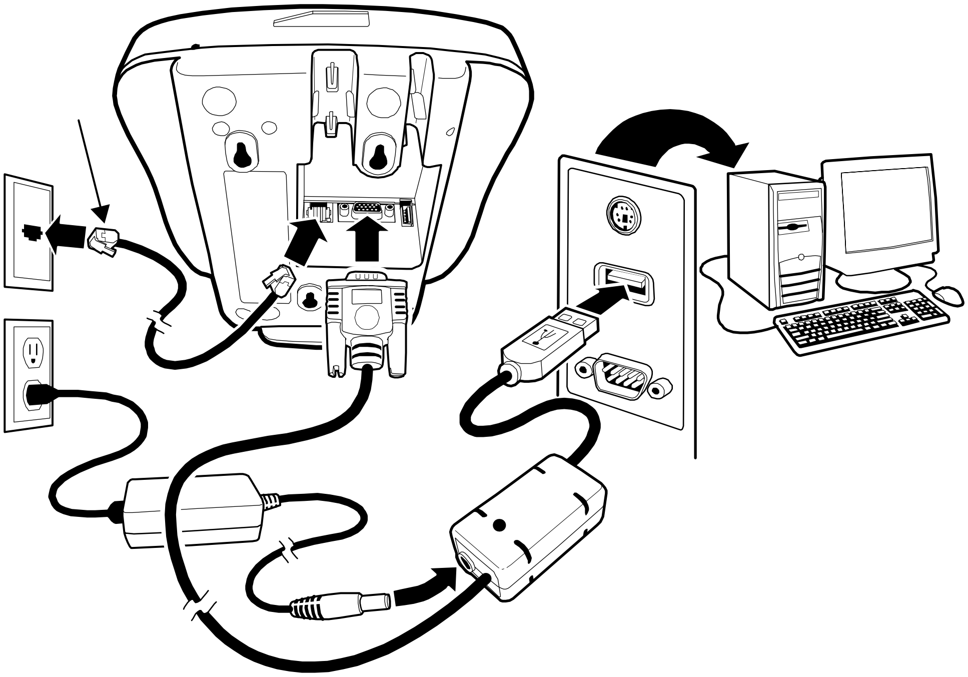
For more information about using ActiveSync on your workstation, open **ActiveSync**, then open **ActiveSync Help**.

Wired Ethernet Communication—IK8560E

IK8560E devices contain an ethernet port on the back panel that is compatible with standard 10/100 Base-T ethernet cables with RJ45 connectors on each end. Cables must be purchased separately.



To establish an ethernet connection, simply plug one RJ45 connector into the ethernet port on the device and the other RJ45 connector into your ethernet outlet.



The IK8560E auto-configures the wired ethernet connection when power is applied from the power cable. DHCP is enabled by default; a static IP must be configured manually if the network does not use DHCP.

To test the ethernet connection, tap the Internet Explorer icon on the Desktop Internet Explorer. If the device connects to a network with internet or an intranet web server, the home page should begin loading.

Adding Programs from a Network

However you establish your network connection–ethernet or wireless radio–you can download and install programs from a network.

⚠ *When selecting programs, verify that the version of the program is designed for both Windows CE and your Intel processor. Check both by tapping Start > Settings > Control Panel > System > General tab.*

1. When you have established your network connection, open Internet Explorer and navigate to the web site.

2. Download the program files to your device.
   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, Readme files, or documentation that comes with the program. (Many programs provide special installation instructions.)

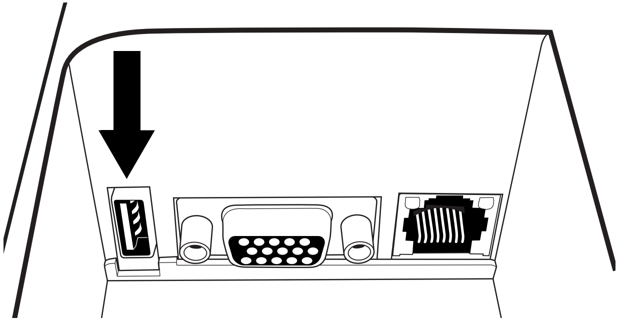
4. On the Desktop, double-tap the **My Device** icon My Device.

5. Tap the installation file. The installation wizard begins.

6. Follow the directions on the screen to install.

USB Host Port

All IK8560 devices have a 4-pin USB 1.1 host port on the back panel that supports USB communication with USB 1.1 and backward-compatible USB 2.0 devices. All data communication occurs at USB 1.1 speeds.



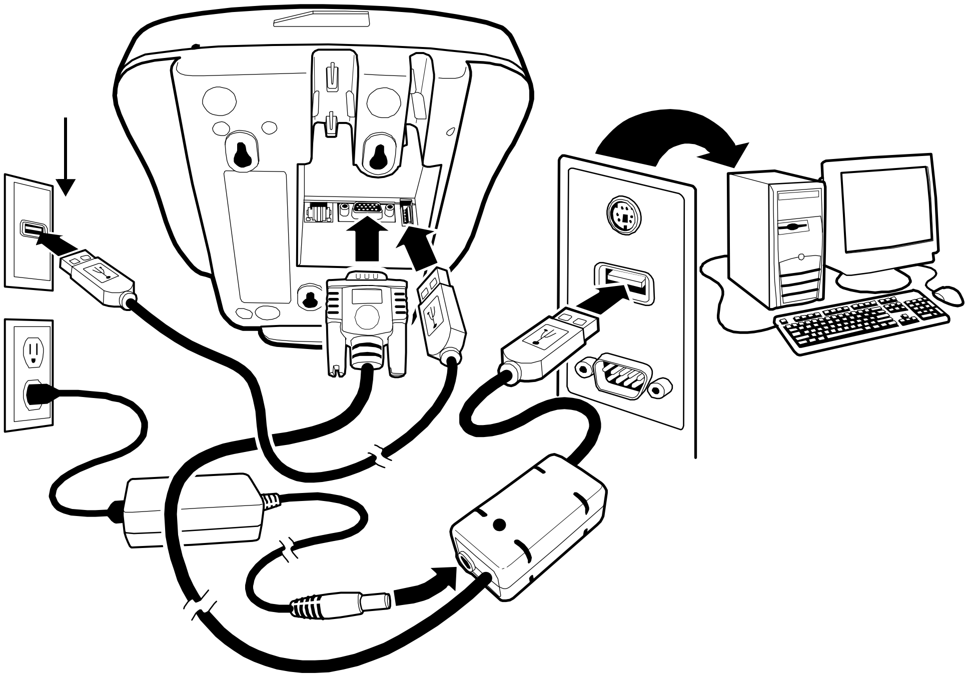
Multiple USB devices can be accommodated by plugging a USB HUB into the USB Host port. The IK8560 can support the following USB peripherals:

- Mouse
- Keyboard
- Mass Storage

Note: The IK8560's USB host port can support a maximum current output of 500mA. If all of your USB devices together require more power, attach them to a self powered hub, and plug the hub into the IK8560.

Connecting the IK8560

To connect the IK8560 to other devices via USB, simply use a standard USB cable to plug one end into the USB host port and the other end into the USB device. The IK8560 auto-configures to USB when power is applied.



5

IK8560C—Wireless LAN with 802.11b

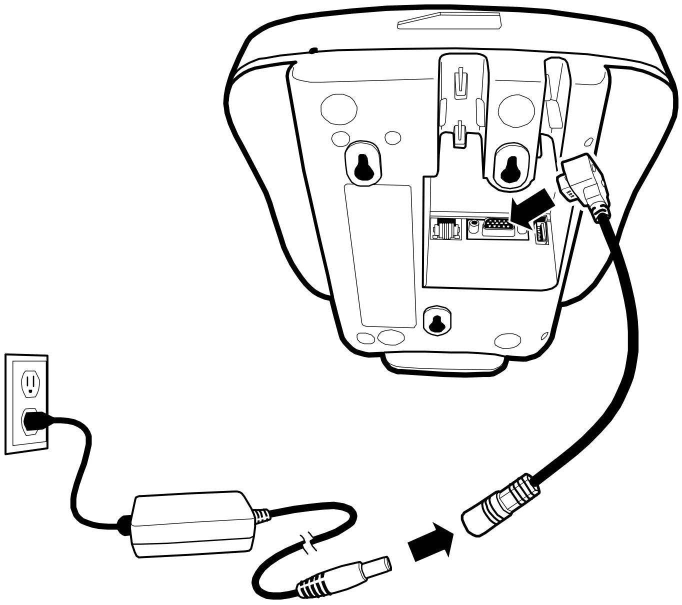
Overview

The IK8560C has an on-board 2.4 GHz 802.11b WLAN (Wireless Local Area Network) radio that uses Direct Sequence Spread Spectrum (DSSS) technology. The signal is spread continuously over a wide frequency band at a data rate of up to 11 Mbps. The radio is interoperable with other 802.11b Wi-Fi-compliant products including Access Points (APs), PCs via PC card adapters and other wireless portable devices.

Note: *The IK8560C does have an RJ45 jack on the back panel; however IK8560C devices do* ***not*** *support wired ethernet communication! Only IK8560E devices contain a functional ethernet controller that allows ethernet communication.*

Cable Options

There is a six inch L connector power cable that you can use to power the IK8560C.



Configuring the 802.11b Radio

On IK8560C devices, the 802.11b driver is enabled during the boot process, which means that the radio is transmitting an RF signal. However, you need to configure the radio in Windows CE to connect to your wireless LAN.

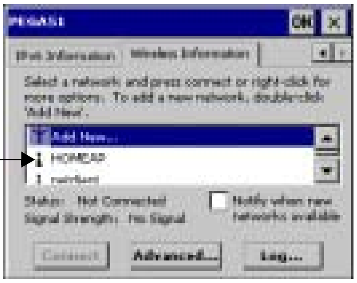
You can configure the radio via Windows CE using wireless zero config…

802.11b with Wireless Zero Config

sample text

1. Open the start screen and tap the radio connection icon in the command bar .
   (The icon looks like this when the radio is not connected.)

2. On the window that opens, tap the **Wireless Information** tab.



PEGAS1

Select a network and press connect or right-click for more options. To add a new network, double-click 'Add New'.

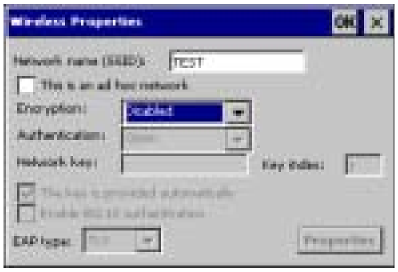
Add New...
HOMEAP
[illegible]

Status: Not Connected
Signal Strength: No Signal

□ Notify when new networks available

The enabled 802.11b radio automatically finds the available networks in the area and displays them in the list.

3. At the top of the list, double-tap **Add New…**



Wireless Properties

Network name (SSID): TEST

□ This is an ad hoc network

Encryption: Disabled

Authentication: Open

Network key:

Key index: 1

☑ The key is provided automatically

□ Enable 802.1X authentication

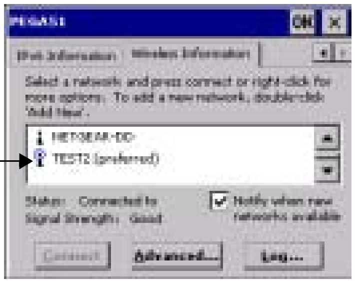
EAP type: TLS

Note: Double-tap one of the found networks to configure it. The Wireless Properties window opens displaying parameters from the network.

4. Type in the **SSID** of the AP or network device you want the device to connect to.

5. Select the **Encryption** and **Authentication** methods.
   See Disabling Encryption on page 5-2.

6. Tap **OK**. You are returned to the Wireless Information tab.



PEGAS1

Select a network and press connect or right-click for more options. To add a new network, double-click 'Add New'.

NETGEAR-DD
TEST2 (preferred)

Status: Connected to
Signal Strength: Good

☑ Notify when new networks available

- The SSID just entered selected as the preferred network connection. Preferred networks are those networks that the device connects to as part of the wireless LAN.
- The device attempts to connect to the SSID automatically and displays the connection **Status** and **Signal Strength**.

Disabling Encryption

To disable encryption, you must first select **Open** or **Shared** as the **Authentication**, then go back up to **Encryption** and select **Disabled**.

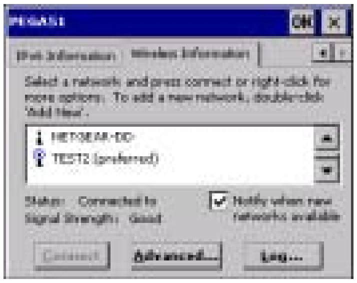
You can disable encryption for Open and Shared Authentications only. **Disabled** does not appear as an option in the **Encryption** drop-down list until **Open** or **Shared** is selected as the **Authentication** method.

Editing Radio Configuration

When the radio is configured and connected to the wireless LAN network, the following icon appears in the taskbar: . Double-tap this icon to access the Wireless Information Tab (see page 5-3). Then, double-tap a preferred network in the list and edit the parameters on the Wireless Properties Window (see page 5-5).

Wireless Information Tab

The wireless information tab manages your 802.11 network connection.



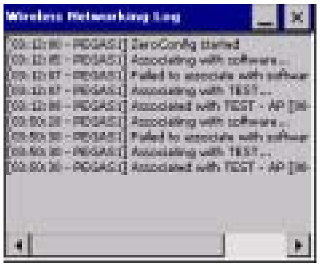
PEGAS1

Select a network and press connect or right-click for more options. To add a new network, double-click 'Add New'.

NETGEAR-DD
TEST2 (preferred)

Status: Connected to
Signal Strength: Good

☑ Notify when new networks available

Field	Description
Network List	Because the 802.11b radio is enabled and transmitting by default, every time you open this window, the device searches for available networks and displays the results in this list.
ⅰ	Networks with this icon have not been configured. To configure a network, double tap the name of the network connection. The Wireless Properties window opens with the name entered in the SSID field; see Wireless Properties Window on page 5-5.
⚲	Networks with this icon have been configured. They will have “preferred” after the name as well. You determine the order of preferred networks on in Advanced Wireless Settings (see page 5-6).
Status	Displays the connection status of the device. • **Scanning**—Displays when the device is attempting to connect to a selected network. • **Associating**—Displays when the device is connecting to a selected network. • **Failed to connect**—Displays when the device fails to connect to a selected network. After failing, the device attempts to connect to the next preferred network. • **Connected to** [Network Name]—The device is connected to the network name listed.
Signal Strength	Indicates the strength of the signal.
Notify when new networks available	If you select this option, the device continually searches for networks. A popup window appears (in any open application) notifying you when the device finds a new network.
Connect	Select a network in the list and tap this button to manually connect the device to the network. If the network has not been configured, tapping this button opens the Wireless Properties Window (page 5-5) with the name entered as the SSID.
Advanced	Opens Advanced Wireless Settings (see page 5-6).
Log	Opens a log, which provides you with a list of radio activity since the last cold boot.  Wireless Networking Log [03:12:00 - PEGAS1] ZeroConfig started [03:12:05 - PEGAS1] Associating with software... [03:12:07 - PEGAS1] Failed to associate with softwar [03:12:07 - PEGAS1] Associating with TEST... [03:12:08 - PEGAS1] Associated with TEST - AP [00- [03:50:30 - PEGAS1] Associating with software... [03:50:30 - PEGAS1] Failed to associate with softwar [03:50:30 - PEGAS1] Associating with TEST... [03:50:30 - PEGAS1] Associated with TEST - AP [00-

Preferred Networks

When a network is selected as a preferred network, the device searches for and connects to that network automatically, even after a warm boot. During that warm boot, the device enables the radio. When the warm boot is complete, the radio searches for the preferred networks and connects.

⚠ Preferred network information is stored in RAM memory and erased during cold boots. The device cold boots automatically when power is removed and then re-applied.

To Edit a Preferred Network

Double-tap the network name in the list and the Wireless Properties window opens. Make your edits and tap **OK** to save.

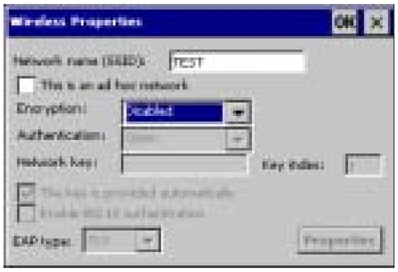
To Delete a Preferred Network

Tap **Advanced**, select the network name in the Preferred Networks list, and tap **Delete**.

Deleting in this way does not delete the network connection. Instead, it deletes the connection's preferred status. The device will search for and retrieve all available networks when you open the Wireless Information Tab (page 5-3). You can select the network and make it a preferred network again, with the same name or a different name.

Wireless Properties Window

Open the Wireless Properties window by double-tapping an available network on the Wireless Information Tab (page 5-3).



Network name (SSID): TEST

□ This is an ad hoc network

Encryption: Disabled

Authentication: Open

Network key:

Key index: 1

☑ The key is provided automatically

□ Enable 802.1X authentication

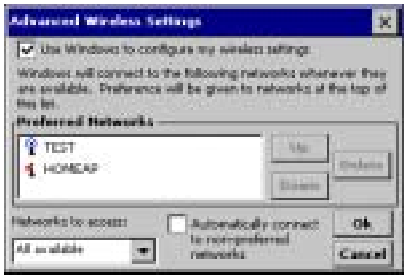
EAP type: TLS

The SSID appears in the field automatically. Other fields on the window are usually completed based on information from the available network. Certain fields may auto-fill or auto-select based on the criteria you enter in other fields.

Field	**Description**
Network Name (SSID)	This is the name of the network. SSID (Service Set IDentifier) is the name assigned to a wireless Wi-Fi network. All devices must use this same, case-sensitive name to communicate, which is a text string up to 32 characters long. When you double-tap on a network name of one of the found networks on the Wireless Information tab, its SSID appears here automatically. Don’t change the name.
This is an ad hoc network	This option identifies the wireless LAN as an ad hoc network, which is a peer-to-peer wireless network that transmits from device to device without using a central base station (access point). Routing from one node to another on such a network requires an on-demand routing protocol, which generates routing information only when a station initiates a transmission.
Encryption	Select the encryption method from the following options: • Disabled—Select this option to disable encryption for Open or Shared authentications. This information is often read from the selected network. • TKIP (available only for WPA and WPA-PSK Authentications) • WEP
Authentication	Select the authentication method from the following options: • Open • Shared • WPA • WPA-PSK
Network key & Key index	If required for your LAN or encryption method, enter the network key and key index. These fields may be disabled based on the selected network.
The key is provided automatically	Select this option if the key is provided automatically. This option may auto-select based on network criteria entered previously.
Enable 802.1X authentication	Select this option to enable the specified authentication method for the 802.11b radio. This option may auto-select based on network criteria entered previously.
EAP type	Select the EAP type from the following options: • TLS • MD5 • PEAP
Properties	This button provides access to certificate settings. This button may be disabled based on the selected network.

Advanced Wireless Settings

Tap **Advanced** on the Wireless Information Tab (page 5-3) to open Advanced Wireless Settings.



Advanced Wireless Settings

☑ Use Windows to configure my wireless settings

Windows will connect to the following networks whenever they are available. Preference will be given to networks at the top of this list.

Preferred Networks

TEST
HOMEAP

Networks to access: All available

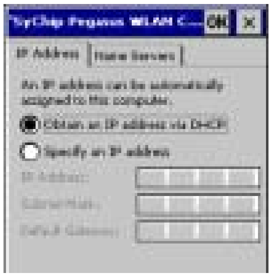
□ Automatically connect to non-preferred networks

On this window, you determine the sequence of connection attempts the device makes when accessing the wireless LAN.

Field	Description
Use Window to configure my wireless settings	When selected, this option tells the device to use these tools to configure the radio. This option is disabled by default, which tells the device to use the Meetinghouse AEGIS Client to configure the radio; for details, see 802.11b Wireless Security on page 5-8.
Preferred Networks list	This is a list of all the networks you've configured. They appear in the exact order the device uses to connect to the wireless LAN. This icon appears next to a preferred network the device cannot connect to.
Up **Down**	Tap **Up** to move a selected network up one place. Tap **Down** to move a selected network down one place. The network at the top will be the default network. If the device fails to connect, it will try to connect with the next preferred network in the list.
Delete	Select a network in the list and tap **Delete** to delete it.
Networks to access	The item selected in this drop-down list determines which type of network the device searches for after the radio is enabled during bootup. • **All available**—The device searches for all available wireless networks. This is selected by default. • **Only access points**—The device searches only for access points. • **Computer-to-computer**—The device searches only for other devices.
Automatically connect to non-preferred networks	This option is not selected by default so that the device only attempts to connect to preferred networks. If selected, the device attempts to connect to all available networks.
OK	Tap to save changes made on this window.
Cancel	Tap to close the window without saving changes.

IP Addresses

To see the IP settings for the 802.11b radio, tap **Start** > **Settings** > **Network and Dial-up Connections**. Double-tap the radio icon . The IP Address tab window opens displaying the current IP settings for the 802.11b radio.



An IP address can be automatically assigned to this computer.

● Obtain an IP address via DHCP

○ Specify an IP address

IP Address:

Subnet Mask:

Default Gateway:

By default, the 802.11b radio uses Dynamic Host Configuration Protocol (DHCP), which automatically assigns temporary IP addresses to client stations logging onto an IP network. It eliminates having to manually assign permanent "static" IP addresses.

If you want to use a static IP address, select **Specify an IP address** and enter the parameters in the fields that activate below as well as the Name Servers tab.

802.11b Wireless Security

The IK8560 contains the Meetinghouse AEGIS Client®, a 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 APs and authentication servers including Microsoft's IAS and Cisco's ACS.

The Client uses public key authentication and encryption between Wireless APs (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.

Supported Protocols

The Client supports the Extensible Authentication Protocol (EAP) - RFC 2284.

Supported authentication methods:

- 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 Server 1.1.4 using MD5, TLS, TTLS, LEAP and PEAP
- Cisco ACS 3.2 using MD5, TLS, LEAP and PEAP

Required Network Configuration Information

Because the Client accesses 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. Therefore, make sure you have the correct network server parameters on hand when you configure the client.

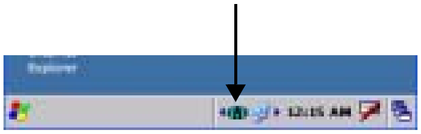
Saving Your Settings

⚠ Network setup information for the client is stored in the registry. To make sure that network information persists through hard resets (i.e., power cycles), back up the registry after you complete network setup.

After settings are saved, tap **Start** > **Power Tools** > **RegBackup** .

Opening the Client

Double tap the icon in the command bar.



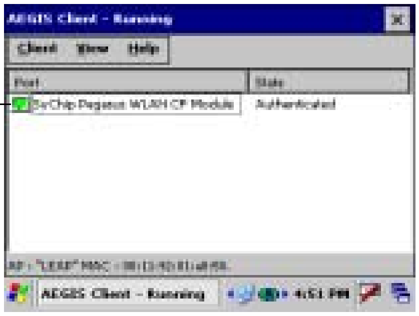
Color Indicators

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 the icon is not yellow, red or green, 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.

Main Window

Double tap on the icon in the command bar to open the Client 🟢. The main screen opens displaying a list of ports on the system's network interface cards. This is the main window.



Port	State
ZyChip Pegasus WLAN CF Module	Authenticated

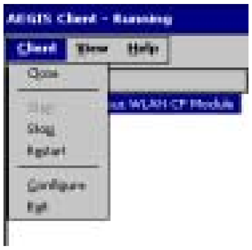
Port Status Icon

The main screen contains a port status icon to the left of each port. The color of the port status icon changes as the port starts authentication, negotiates with the AP 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.

The colors of the port status icon are the same as the color of the icon in the command bar. For details about what each color means, see Color Indicators on page 5-9.

Client Menu

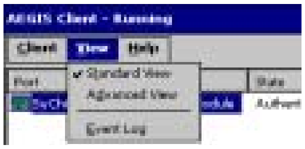
On the main window, tap the **Client** menu.



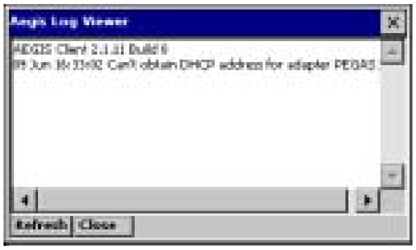
Menu Item	Description
Close	Closes the Client's interface, while leaving the client running.
Start/Stop	Starts or stops 802.1X authentication. After you finish the initial configuration, tap the network interface and tap **Start.** If the port is already active, tap **Stop** first, then **Start** to force the program to read the new configuration file.
Restart	Same as a Stop followed by Start. Select this menu item when you receive a message that a restart is necessary.
Configure	Opens the client authentication screens; see Configuring Client Authentication on page 5-13.
Exit	Terminates the client, which stops the 802.1X protocol.

View Menu

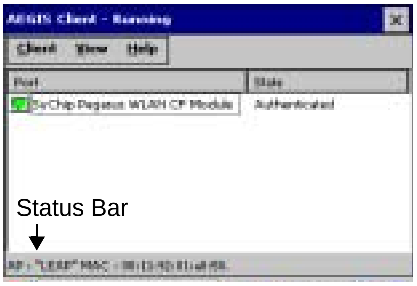
To access the View menu, tap **View**.



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

Menu Item	Description
Event Log	Displays the event log in a custom viewer. The Event Log is a text file that contains system information; each entry is listed sequentially with a time/date stamp and text message. Tap **Refresh** to query the system again and update the log file while you are reading it. If the file gets too large, old entries are automatically deleted. Logging parameters are set on the System Tab (see page 5-15)  AEGIS Client 2.1.11 Build 6 09 Jun 16:33:02 Can't obtain DHCP address for adapter PEGAS

Status Bar



Port	State
🟩 ...Chip Pegasus WLAN CF Module	Authenticated

AP : "LEAP" MAC : 00:13:[illegible]

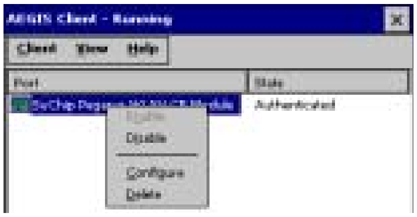
The status bar at the bottom of the main screen indicates the connection status between the network card and the AP.

Depending on the status of connectivity, the status bar displays one of the following:

- Not Associated
- AP : [AP's SSID] MAC : [AP's BSSID].

Port Menu

The Port menu enables you to configure the port. On the main screen, tapping once on a port opens a popup menu.



Menu Item	Description
Enable **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 Start/Stop on page 5-10); however, both actions are required for the Client to work.
Configure	Opens the port configuration screen; see Configuring Client Authentication on page 5-13.
Delete	Removes an adapter from the port list. Selecting Delete has not effect on the

Setup Screens

Use the following navigation aid to examine the configuration options for each set of screens:

Configuring Client Authentication (see page 5-13)

- User Tab (see page 5-13)
- System Tab (see page 5-15)
- Server Tab (see page 5-16)

Configuring a Port (see page 5-17)

- Wireless Networks Tab (see page 5-17)
- Protocol Tab (see page 5-18)

Configuring a Network (see page 5-19)

- Profile Info Tab (see page 5-19)
- WEP Mgmt Tab (see page 5-20)
- WPA Settings Tab (see page 5-21)

Saving Your Settings

⚠ Network setup information for the client is stored in the registry. To make sure that network information persists through hard resets (i.e., power cycles), back up the registry AFTER you complete network setup. You can also export the registry to save it for future use on multiple devices.

To back up the registry, tap **Start** > **Power Tools** > **RegBackup** RegBackup .

To export the registry, tap **Start** > **Power Tools** > **RegEdit** RegEdit > **File** > **Export**.

Configuring Client Authentication

Each user account needs to define the protocol and the credentials used to authenticate a user. When you start and stop on a port, you are enabling and disabling the authentication established here.

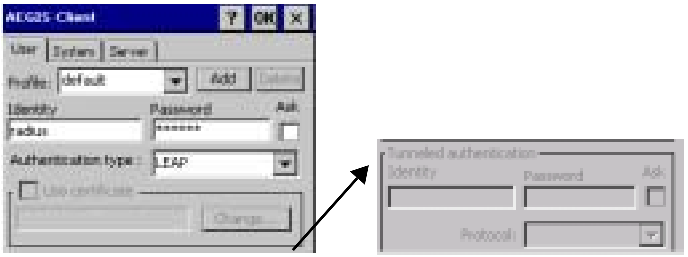
Note: Fields will be grayed out if not relevant to the selected protocol.

On the main screen, tap **Client** > **Configure**. Complete the User (see page 5-13), System (see page 5-15), and Server (see page 5-16) tabs.

⚠ The configuration screens are in portrait orientation, which means that a portion of the screen is below the command bar at the bottom. To access the rest of the screen, tap and hold on a point on the right side of the window that is not an active part of the screen (e.g., a button or a field) and drag the screen up. After you complete your tasks on the lower portion of the window, you must drag the window back down so that you can tap **OK** to save changes.

User Tab

Enter the credentials used to authenticate a user.



Profile: default

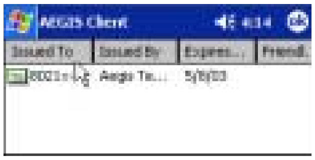
Identity: radius

Password: ******

Ask: □

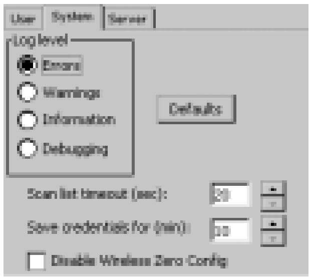
Authentication type: LEAP

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. • 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.
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. 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.

Field	Description
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.  AEGIS Client 4:14 ok Issued To · Issued By · Expires... · Friendl... 8021x... · Aegis Te... · 5/8/03 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. To appear in this list, certificates must be installed in the system; see Installing Certificates on page 5-22. The **Issued to** column should match the **Identity** field and the user ID on the authentication 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. 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. 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.
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 • MS-CHAP-V2 The following protocols are currently supported for PEAP: • EAP-MS-CHAP-V2 • TLS/SmartCard • Generic Token Card (EAP-GTC)

System Tab

Define logging settings and the port manger timeout period.



Log level

● Errors
○ Warnings
○ Information
○ Debugging

Scan list timeout (sec): 20

Save credentials for (min): 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. For more information, see Logging on page 5-15.
Defaults button	Tap this button to return log settings to the default settings.
Scan List Timeout	The time interval at which the Client polls the ports. This value should not be changed from the 10-second default unless technical support advises you to do so.
Save Credentials for (min)	The amount of time the Client saves credentials.
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 need to do a RegBackup and then power cycle the device whenever this setting is changed.

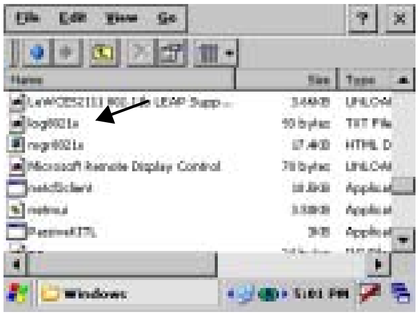
Logging

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).

In the text file, the format of the entries is: **Time StampMessage Text**

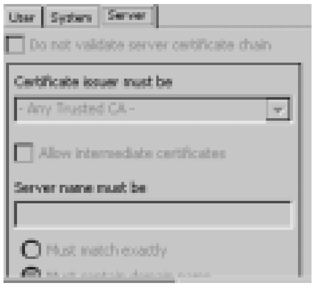
Note: To see an event log on the screen, tap View > Event Log (see page 5-11).

If you wish to start with a blank file or clear the event log, close the Client (so that the icon no longer appears in the command bar) and delete the log file (log8021x) in WIndows Explorer. When you restart the Client, a new log file is created.



Server Tab

The Server tab controls 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. The Client uses this information to verify that the Client is communicating with a trusted server.

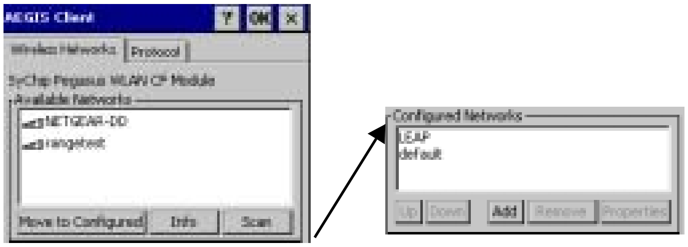

User
System
Server
□ Do not validate server certificate chain
Certificate issuer must be
- Any Trusted CA -
□ Allow intermediate certificates
Server name must be
○ Must match exactly
● Must contain domain name

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 and enables unspecified certificates to be in the server certificate chain between the server certificate and the certificate authority selected in the Certificate issuer must be field. When selected, this option 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.
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).

Configuring a Port

On the main screen, tap and hold on a port and tap **Configure**. Complete the Wireless Networks Tab (see page 5-17) and the Protocol Tab (see page 5-18).

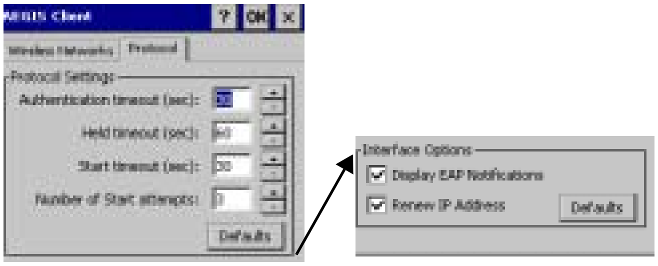
Wireless Networks Tab



Field	Description
Available Networks	Displays the networks the device recognizes as available to connect to.
Move to Configured	Activates after the available networks have been retrieved. Select the network you wish to connect to, and tap Move to Configured. This selects the network.
Scan	Displays a list of networks broadcasting their availability. You can also attach to networks that are not broadcasting.
Configured Networks	Displays the configured network profiles saved in the device.
default	This is the default network configuration that installs when the Client installs. This network profile associates with any network. If you are in a location with only one AP (or more than one AP that attaches to the same network), the default profile may be sufficient without requiring the selection of a specific network or networks. If default is last in the list, it can act as a wildcard if the device is out of range of the primary networks (listed first). Do NOT place **default** at the top or middle of the list if you are connecting to other networks! If default is any place other than last, connection to the other list entries is never attempted.
Up & Down	Moves a selected network up or down one place in the list.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.
Add	Manually adds a network to the Configured Networks list if the AP does not broadcast its SSID or you are pre-configuring the client for an AP that is not currently in range. For details, see Configuring a Network on page 5-19.
Remove	Removes a selected network from the list.
Properties	Displays the properties of the network selected in the list. Tap this button to edit existing wireless network configurations. For details, see Configuring a Network on page 5-19.

Protocol Tab

The Protocol tab configures parameters that apply to all the networks the selected port connects to.



Protocol Settings

Authentication timeout (sec): 30

Held timeout (sec): 60

Start timeout (sec): 30

Number of Start attempts: 3

Interface Options

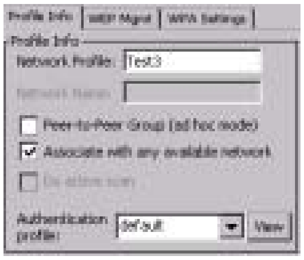
☑ Display EAP Notifications

☑ 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 AP 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.
Display EAP notifications	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	Initiates 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.

Configuring a Network

On the Wireless Networks Tab (see page 5-17), you can tap **Add**.



Network Profile: Test3

Network Name:

□ Peer-to-Peer Group (ad hoc mode)

☑ Associate with any available network

□ Do active scan

Authentication profile: default

Complete the tab windows and tap **OK**.

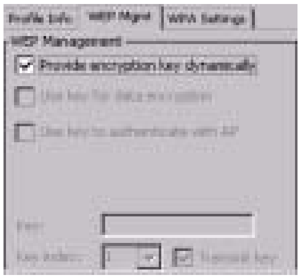
Note: The settings on these tab windows are interrelated. This means that selecting one may disable access to others.

Profile Info Tab

Field	Description
Network Profile	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 AP. If the AP broadcasts its SSID, then this value is retrieved from the Available Networks list and this field is completed automatically. If the SSID does not broadcast, then the field will be active and you must manually enter the value here.
Peer-to-Peer Group	Select this option to have two or more client workstations communicate with each other without the benefit of an AP, otherwise known as ad hoc mode. You should also select **Do Active Scan** and, on the WEP Mgmt tab, select **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 AP (or client, for ad hoc mode) is not broadcasting its SSID. *Note: This option is not available when Associate with any available network is selected.*
Authentication Profile	Select the authentication profile associated with this network and tap **View**. The drop-down list contains client profile names created in the User tab of the client configuration area; see User Tab on page 5-13.

WEP Mgmt Tab

Enter the appropriate WEP parameters for the network.



WEP Management

☑ Provide encryption key dynamically

□ Use key for data encryption

□ Use key to authenticate with AP

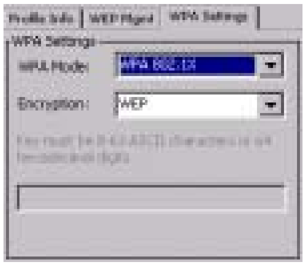
Key:

Key Index: 1 ☑ Transmit key

Field	Description
Provide encryption key dynamically	This option is selected by default. The other WEP settings on this page are disabled to enable dynamic encryption. Selecting this option also enables WPA; the WPA Settings tab appears. To enter a custom WEP, de-select this option. The other fields become active and the WPA Settings tab no longer appears.
Use key for data encryption	Select this option to manually enter a WEP key (in the Key field) to encrypt your data to the AP.
Use key to authenticate with AP	Selecting this option toggles the WEP authentication mode between Open and Shared. When selected, the WEP key (entered in the Key field) is used when clients authenticate with the AP via a challenge/response mechanism (Shared). When not selected, the only authentication performed is to check that a client's SSID setting matches the SSID of the AP (Open).
Key	In this field, enter the WEP key to use for data encryption or authentication to the AP. **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.
Key Index/Transmit Key	This 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 AP. 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

This tab controls the WPA settings. This tab window is available only if **Provide encryption key dynamically** is selected on the WEP Mgmt tab is selected.



WPA Mode: WPA 802.1X

Encryption: WEP

Key must be 8-63 ASCII characters or 64 hexadecimal digits

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.
Encryption	Select the desired encryption. • **WEP**: The least secure of the encryption methods. WEP uses a single encryption key of either 40 or 104 bits. WPA uses a 256 bit Pre-shared key. • **TKIP**: Uses the standard WEP format, but changes the key with every frame for improved security and includes a message integrity capability for determining unauthorized packet insertion. • **AES**: The strongest form of the encryption methods.
PSK pass-phrase	This field activates if you select WPA PSK as the mode. Enter between 8 and 63 characters for your pass phrase. Asterisks appear as you type for increased security.

Installing Certificates

Install certificates with CertAdd, a standalone utility that allows certificates to be selected and installed on the device.

Certificate Requirements

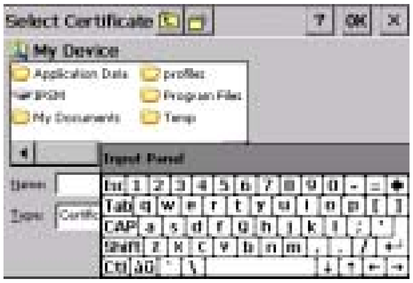
During configuration, you may have specified one or two certificates to use during the authentication process. The specified identity should match the **Issued to** field in the certificate and should be registered on the authentication server (i.e., a RADIUS server) that is used by the authenticator. 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 (CA).

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.

Installing Certificates

*Note: Client or CA certificates can be imported from *.cer (same as *.der), *.p7b, or *.pfx files.*

1. Download the certificate file to the device.
   The location isn't critical, but you may want to create a standard folder for consistency.
2. Go to **Start** > **Programs** > **Meetinghouse Certificate Installer**.



3. Navigate to the certificate location.
4. Tap and hold on a certificate in the list. A pop-up appears asking if you want to install the certificate.
5. 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. • Restart the client: on the main screen tap **Client** > **Restart**. • Perform a soft reset. • If problem continues to persist through all of the above, there may be a hardware failure.
The Client is not attaching to the correct AP.	The **default** network profile instructs the client to attach to the first available AP. 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 5-17.
The Client is failing authentication even though all my information was entered correctly.	1. Verify that the network profile for the AP 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 5-19. • 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 5-19) in the authentication profile. If you are using PEAP or TTLS, the username and password are entered in the Tunneled authentication section.
My AP does not broadcast its SSID. Even though I have manually configured an AP with that name, the Client won't associate with it.	• Make sure that the Network Name field contains the AP’s SSID. • Verify that Do Active Scan is selected on the Profile Info tab; see Do active scan on page 5-19. Otherwise, the Client will not attempt to find the AP.
I am authenticated, but I don't get an IP address through DHCP.	• On the main screen, tap on the port, tap **Configure** on the popup menu, and select the **Protocol** tab. Verify that **Renew IP Address** is selected; see page 5-18. • Make sure that radio is configured for DHCP and not assigned a static IP address.
I cannot attach to my old network that does not support 802.1x authentication, but is using WEP encryption.	• On the Wireless Networks tab, verify that the SSID is at the top of the Configured Networks list so it’s accessed first. • Tap the port and select **Configure**. • On the Wireless Networks tab, select the SSID and tap **Properties**. • On the Profile Info tab, select **Do active scan**. • On the WEP Mgmt tab, select **Use key for data encryption**. • Enter the WEP **Key**; see Key on page 5-20. Tap **OK**. • On the main screen, tap **Client** > **Restart** to restart the Client. • The Client connects; wait for the main screen to update. • When the connection is complete, the port status indicator reads "Associated" instead of "Authenticated." However, the log file will read "Entered AUTHENTICATED state."
I made changes, but they do not appear to have taken effect.	Always tap **OK** before exiting a screen you have changed. Then, on the main window, tap **Client** > **Restart** to restart the Client.

Advice and Workarounds

Issue	Possible Causes and Solutions
How do I enable peer-to-peer (ad-hoc) mode to have two clients communicate without an AP?	• 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.

6 Imaging

Overview

The IK8560 uses Adaptus Imaging Technology™ with an integrated Hand Held Products 5100 Standard Range (5100SR) image engine. When the IK8560 is powered the external illumination LEDs are always enabled providing the required illumination for the 5100SR image engine; however the engine may only be enabled for scanning under software application control. Please refer to the IK8560 SDK on line help for details on connecting to and using the IK8560's integrated scan engine.

The included Scan Demo (see page 6-4) enables the image engine for use in the Scan Demo only.

Supported Bar Code Symbologies

The 5100SR image engine in the IK8560 supports the following bar code symbologies:

- Australian Post
- Aztec Code
- Aztec Mesas
- British Post
- Canadian Post
- Codabar
- Codablock F
- Code 11
- Code 39
- Code 49
- Code 93 and 93i
- Code 128
- Data Matrix
- EAN-8
- EAN-13
- EAN•UCC Composite
- Interleaved 2 of 5
- ISBT 128
- Japanese Post
- KIX (Netherlands) Post
- MaxiCode
- MicroPDF417
- MSI
- OCR
- PDF417
- Planet Code
- Plessey Code
- Postnet
- QR Code
- Reduced Space Symbology (RSS-14, RSS Limited, RSS Expanded)
- Straight 2 of 5 IATA
- TCIF Linked Code 39 (TLC39)
- UPC-A
- UPC-E
- UPC-E1

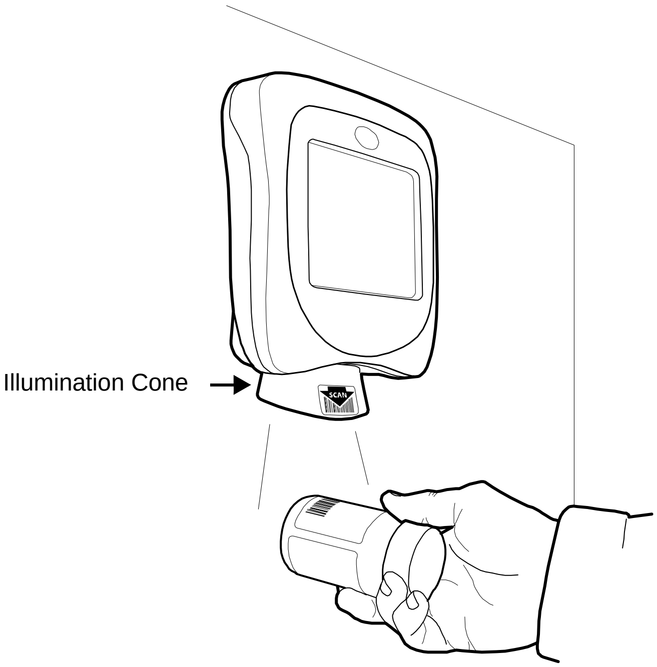
Default Bar Code Symbologies

The IK8560 defaults to the following linear bar code symbologies:

- UPC-A
- UPC-E
- EAN/JAN
- Code 128
- Interleaved 2 of 5
- Code 39
- Codabar
- MSI
- PDF417
- Plessey Code
- RSS-14

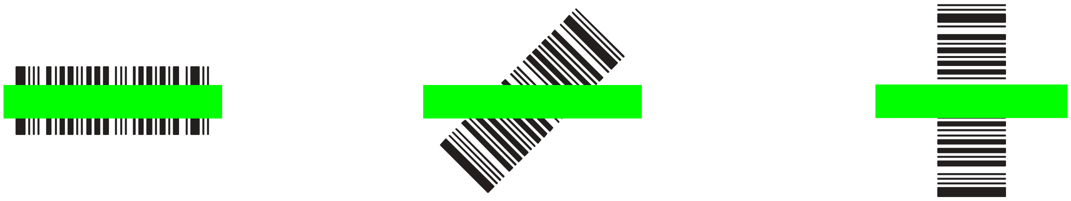
Scanning a Bar Code

If you are running a software application, such as the Scan Demo, that accepts bar code information, simply slide a bar code underneath the illumination cone. The IK8560 beeps on successful decoding.



Omni-Directional Aiming

The IK8560 supports omni-directional aiming in two of the three optimal imaging modes

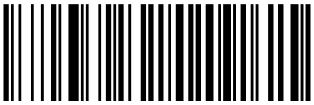


Omni-directional aiming means the bar codes label can be read if placed under the illumination cone in any orientation.

Sample Bar Codes

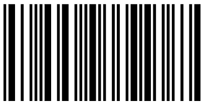
The following are bar code samples you can use with the Scan Demo to verify decoding on the IK8560:

Sample Code 128



Readout: “Code 128”

Sample Codabar



Readout: “13579”

Depth of Focus (DOF) Specifications

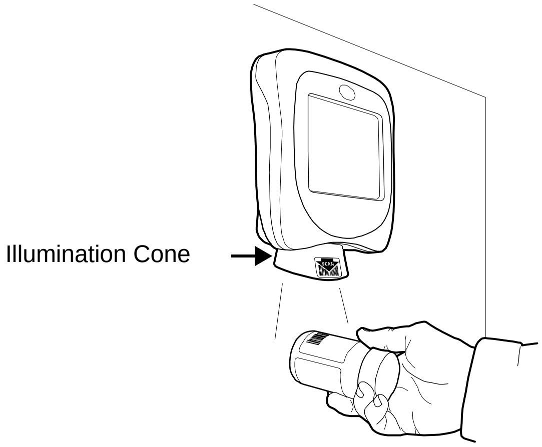
The point of reference for the IK8560 DOF specifications is from the outermost edge of the illumination cone. Ambient light level at 535 Lux.

Code	Near	Far
MaxiCode (35-mil)	Contact	9.95
Data Matrix 15-mil (ECC 200)	0.65”	3.45"
PDF417, ECL4 10-mil	0.05”	5.95"
PDF417, ECL4 8-mil	0.25”	4.95"
PDF417, ECL4 6.6-mil	1.45”	3.2"
Code 39 15-mil	Contact	9.75"
Code 39 10-mil	0.15”	6.15"
Code 39 8-mil	0.45”	4.55"
UPC-A 13-mil, 100%	Contact	9.45"
Postnet	0.95”	2.85"
12-point OCR-A	Contact	8.75"
12-point OCR-B	Contact	7.95"

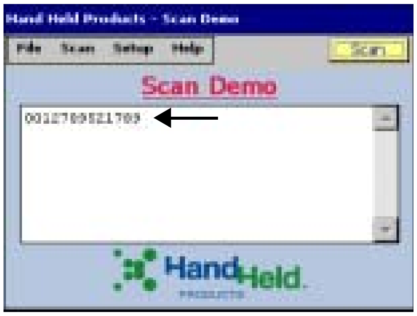
Scan Demo

The IK8560 ships with a sample application called Scan Demo that can be used to demonstrate the scanning capabilities of the IK8560. To launch and use the Scan Demo application please follow the following steps:

1. Tap **Start** > **Programs** > **Demos** and double-tap the **Scan Demo** icon Scan Demo. The Scan Demo window opens and the image engine is activated.
2. Slide a bar code under the illumination cone and tap **Scan**.



3. The device beeps and the bar code data appears on the screen.



00127093521709

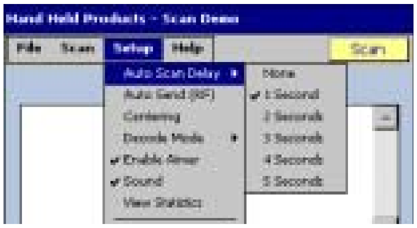
Scanning Options

You can always manually scan the bar code inserted under the illumination cone by tapping the **Scan** button. The Scan menu offers you two additional scan options: Automatic and Continuous.

Automatic Scan

Automatic scan activates the image engine at regular one second intervals. To set the device to automatic scan, tap **Scan** > **Automatic** and the engine begins scanning at one-second intervals. Simply slide a bar code under the illumination cone and wait for the readout to appear on the screen.

One second is the default interval; however, you can customize the interval time by tapping **Setup** > **Auto Scan Delay**.



Select an interval from 1 to 5 seconds. A checkmark appears next to the selected interval. Selecting None causes the engine to scan continuously. To turn off automatic scanning, tap **Scan** > **Automatic** again.

Continuous Scan

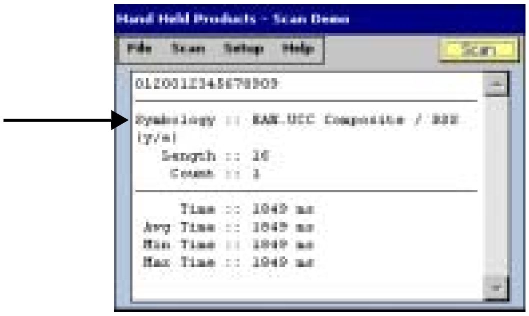
Continuous scan activates the image engine continually, without a pause. To set the device to continuous scan, tap **Scan** > **Continuous** and the engine begins scanning. Automatic scan **must** be turned off before you can activate continuous scan. To turn off continuous scanning, tap **Scan** > **Continuous** again.

Note: If you want to track bar code scans during automatic or continuous scan, enable the scan statistics.

Enabling Scan Statistics

The Scan Demo can record scan statistics for each bar code scanned and for all bar codes scanned in an activated scan session. By default, these statistics do not display on the screen.

To enable scan statistics and activate a scan session, tap **Setup** > **View Statistics**. The Scan Demo begins recording scan statistics beginning with the next bar code scanned. The scan statistics will appear underneath the bar code readout.



```
0120012345678909

Symbology :: EAN.UCC Composite / RSS
(y/n)
   Length :: 16
    Count :: 1

     Time :: 1049 ms
 Avg Time :: 1049 ms
 Min Time :: 1049 ms
 Max Time :: 1049 ms
```

Field	Description
Symbology	The symbology type.
Length	The length of the bar code.
Count	The number of scans completed since scan statistics were enabled. If you complete one scan, this field displays a count of 1 and increases with each additional scan performed.
Time	The number of milliseconds (ms) to decode the bar code.
Note: The following three fields display the cumulative scan statistics from the time that View Statistics was enabled. To reset any of these values to zero, disable the scan statistics.	
Average Time	The average decode time of all bar codes decoded.
Min Time	The shortest decode time of all bar codes decoded.
Max Time	The longest decode time of all bar codes decoded.

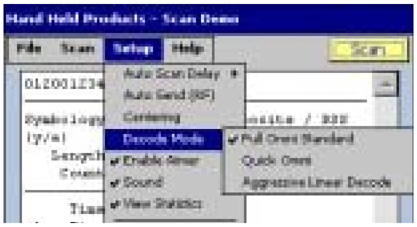
Beeper

By default, the beeper sounds after each successful decoding. To turn off the speaker, tap **Setup** > **Sound**. The beeper will not sound after your next successful scan.

Decode Mode

By default, the Scan Demo decodes in Full Omni Standard mode.

To chose another mode, tap **Setup** > **Decode Mode**. A checkmark appears next to the selected mode.

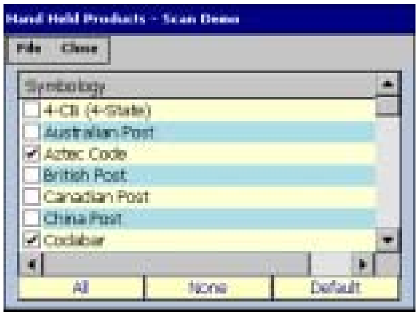


There are three options:

1. **Full Omni/Standard** This is the default scan mode. The image engine looks for any bar code within range.
2. **Quick Omni** The image engine attempts to decode any enabled barcode while searching a reduced area of the image. By searching for a barcode in a reduced area, based around the center of the image, scanning performance may be improved if the barcode label is found close to the center in the captured image used by the scan engine.
3. **Aggressive Linear Decoding**
   The image engine attempts to decode only enabled 1D linear barcodes.

Symbologies

The Scan Demo can decode a bar code only if its bar code symbology is selected in the symbologies list.
To see this list, tap **Setup** > **Symbologies**.



The symbologies with a checkmark are the symbologies currently selected. The Scan Demo defaults to the default bar code symbologies for the IK8560; see Default Bar Code Symbologies on page 6-1.

Enabling and Disabling Symbologies

To enable a symbology, select it in the list. To disable a symbology, de-select it in the list. You can select and de-select more than one symbology at a time. Whe you are done enabling and disabling, tap **Close** and then **Yes** on the confirmation dialog.

In addition to individual, manual selection, the Scan Demo offers you three selection options:

All Selects all the symbologies in the list.

None De-selects all the symbologies in the list; this button de-selects even the default symbologies.

Default Selects only the default symbologies; see Default Bar Code Symbologies on page 6-1.
Use this button to return the Scan Demo to the default symbologies after modifications.

Tap **Close** and save your selections. Tap **Yes** and you are returned to the Scan Demo window. Verify symbology selections by scanning bar codes in the selected symbology(ies) format.

Note: Symbology selections apply only to the Scan Demo, not the image engine in general.

Centering

Centering is a scanning feature that requires the barcode label to be located within a specific area of the imagers field of view in order for the label to be successful decoded. This feature allows the image engine to discriminate between symbols that are located physically close to each other so only one symbol is captured during a decode attempt. Please refer to the SDK's online help for further details on the use of the centering feature.

To enable decode centering, tap **Options** > **Centering**. Centering will be applied to your next scan.

Enabling the Aimer

The 5100SR/SF engine contains a green aiming beam that is disabled by default in the Scan Demo. To enable the aiming beam, tap **Setup** > **Enable Aimer**. A checkmark appears on the menu to indicate that the aiming beam is enabled.

To see the aiming beam, see Omni-Directional Aiming on page 6-2.

Auto-Send

Mounting

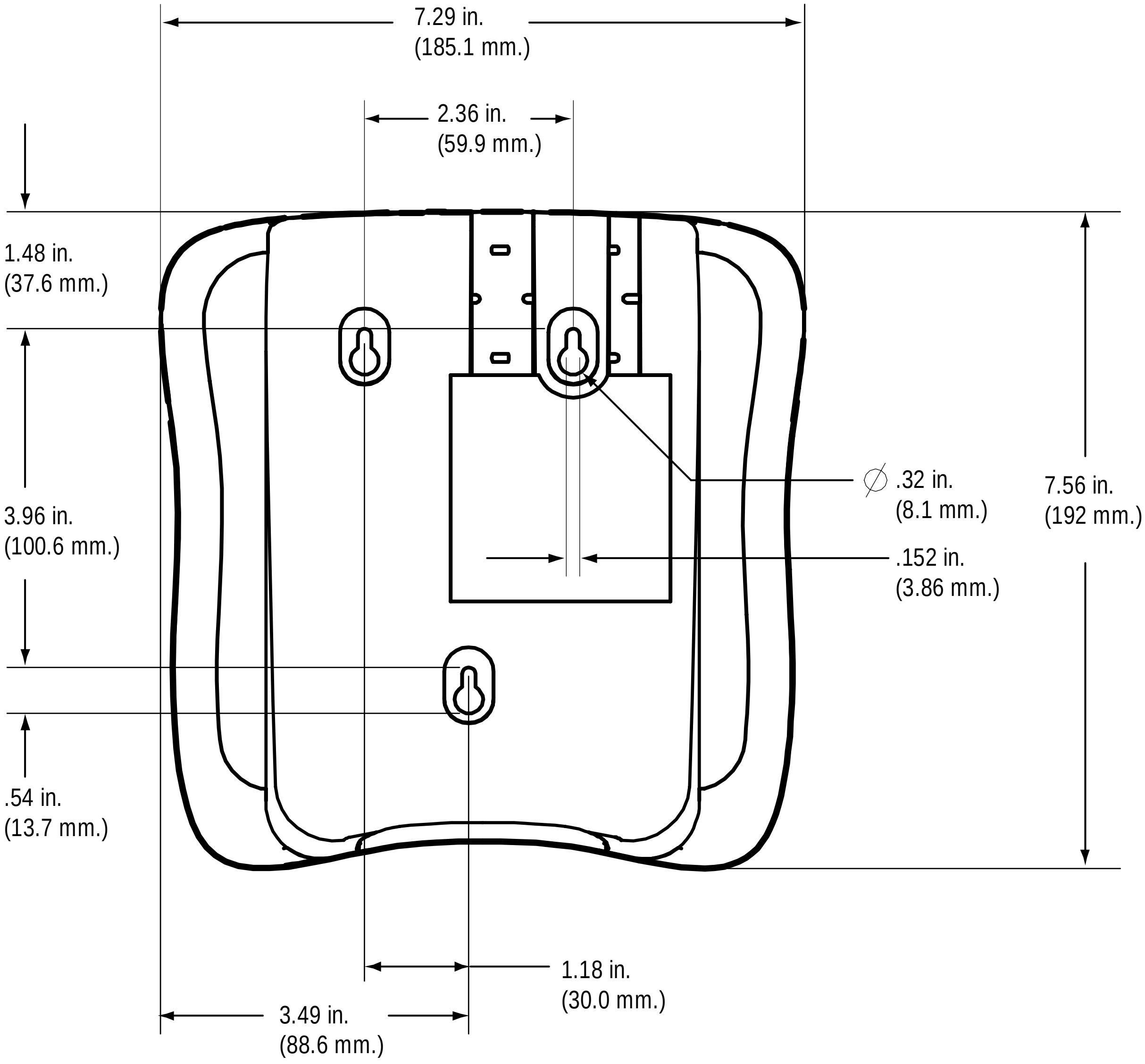
Overview

IK8560 devices are designed for easy mounting to a stable vertical surface. The back panel contains screw slots spaced to fit standard mounting brackets.

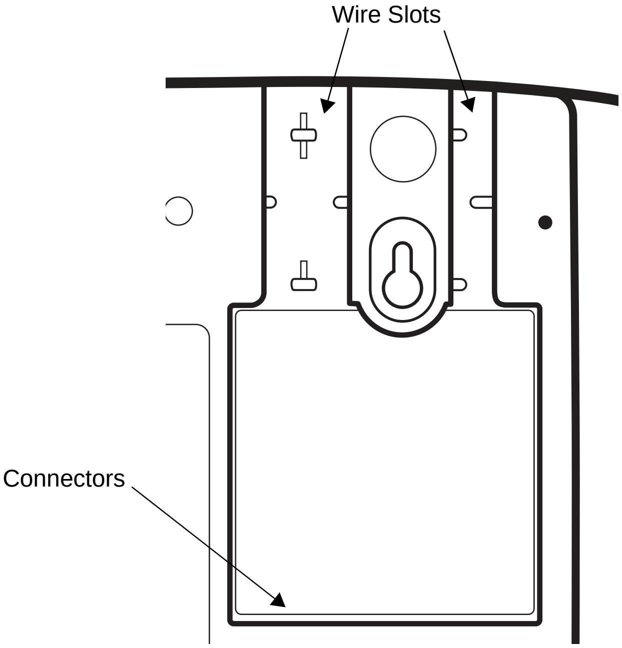
Depending on your environment, you can use a mounting bracket or simply fasten screws directly to the vertical surface and hang the IK8560 on the screws. Make sure to use screws appropriate to the material of the vertical surface, such as wood or drywall.

Back Panel Mounting Dimensions

Use the following dimensions to mount your IK8560 devices.



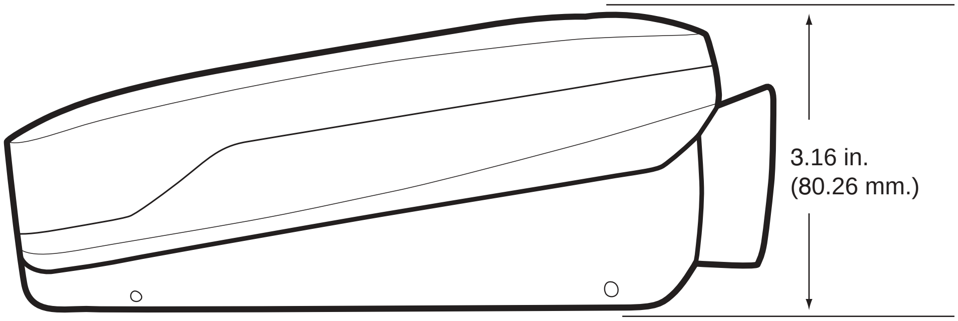
Connector Slots



If you want the IK8560 to lay flat against the mounting surface, make sure that the wires from the connectors are secured in the wire slots.

Side Panel Dimensions

The following graphic shows the depth of the IK8560 at its widest point.



8

Customer Support

Product Service and Repair

Hand Held Products provides service for all its products through service centers throughout the world. To obtain warranty or non-warranty service, return the unit to Hand Held Products (postage paid) with a copy of the dated purchase record attached. Contact the appropriate location below to obtain a Return Material Authorization number (RMA #) before returning the product.

North America

Hand Held Products Corporate Offices
Telephone:(800) 782-4263, option 3
Fax: (704) 566-6015
E-mail: naservice@handheld.com

América Latina

Hand Held Products América Latina
Teléfono: (800) 782-4263, opción 8, opción 4
Teléfono: (704) 998-3998, opción 8, opción 4
Fax: (239) 263-9689
E-mail: laservice@handheld.com

Brasil

Hand Held Products São Paulo
Teléfono: Int+55 (11) 2178-0500
Fax: Int+55 (11) 2178-0502

Hand Held Products Rio de Janeiro
Teléfono: Int+55 (21) 2178-0500
Fax: Int+55 (21) 2178-0505

São Paulo and Rio de Janeiro
E-mail: brservice@handheld.com

México

Hand Held Products México
Teléfono: Intl+52 (55) 5203-2100
Fax: Intl+52 (55) 5531-3672
E-mail: mxservice@handheld.com

Europe, Middle East, and Africa

Hand Held Products Europe
Telephone:+31 (0) 40 29 01 633
Fax: +31 (0) 40 2901631
E-mail: euservice@handheld.com

Asia Pacific

Hand Held Products Asia/Pacific
Telephone:+852-2511-3050
Fax: +852-2511-3557
E-mail: apservice@handheld.com

Japan

Hand Held Products Japan
Telephone:+81-3-5770-6312
Fax: +81-3-5770-6313
E-mail: apservice@handheld.com

Online Product Service and Repair Assistance

You can also access product service and repair assistance online at www.handheld.com.

Technical Assistance

If you need assistance installing or troubleshooting, please call your Distributor or the nearest Hand Held Products technical support office:

North America/Canada:

Telephone:	(800) 782-4263, option 4 (8 a.m. to 6 p.m. EST)
Fax number:	(315) 685-4960
E-mail:	*natechsupport@handheld.com*

América Latina:

Teléfono:	(800) 782-4263, opción 8, opción 3
Teléfono:	(704) 998-3998, opción 8, opción 3
E-mail:	*latechsupport@handheld.com*

Brasil

São Paulo

Teléfono:	Int+55 (11) 2178-0500
Fax:	Int+55 (11) 2178-0502

Rio de Janeiro

Teléfono:	Int+55 (21) 2178-0500
Fax:	Int+55 (21) 2178-0505

São Paulo and Rio de Janeiro

E-mail:	*brtechsupport@handheld.com*

México

Teléfono:	(800) 782-4263, opción 8, opción 3
Teléfono:	(704) 998-3998, opción 8, opción 3
E-mail:	*latechsupport@handheld.com*

Europe, Middle East, and Africa:

Telephone-	
European Ofc:	Int+31 (0) 40 79 99 393
U.K. Ofc:	Int+44 1925 240055
E-mail:	*eutechsupport@handheld.com*

Asia Pacific:

Telephone:	Int+852-3188-3485 *or* 2511-3050
E-mail:	*aptechsupport@handheld.com*

Online Technical Assistance

You can also access technical assistance online at www.handheld.com.

Limited Warranty

Hand Held Products, Inc. ("Hand Held Products") warrants its products to be free from defects in materials and workmanship and to conform to Hand Held Products' published specifications applicable to the products purchased at the time of shipment. This warranty does not cover any Hand Held Products product which is (i) improperly installed or used; (ii) damaged by accident or negligence, including failure to follow the proper maintenance, service, and cleaning schedule; or (iii) damaged as a result of (A) modification or alteration by the purchaser or other party, (B) excessive voltage or current supplied to or drawn from the interface connections, (C) static electricity or electro-static discharge, (D) operation under conditions beyond the specified operating parameters, or (E) repair or service of the product by anyone other than Hand Held Products or its authorized representatives.

This warranty shall extend from the time of shipment for the duration published by Hand Held Products for the product at the time of purchase ("Warranty Period"). Any defective product must be returned (at purchaser's expense) during the Warranty Period to Hand Held Products' factory or authorized service center for inspection. No product will be accepted by Hand Held Products without a Return Materials Authorization, which may be obtained by contacting Hand Held Products. In the event that the product is returned to Hand Held Products or its authorized service center within the Warranty Period and Hand Held Products determines to its satisfaction that the product is defective due to defects in materials or workmanship, Hand Held Products, at its sole option, will either repair or replace the product without charge, except for return shipping to Hand Held Products.

EXCEPT AS MAY BE OTHERWISE PROVIDED BY APPLICABLE LAW, THE FOREGOING WARRANTY IS IN LIEU OF ALL OTHER COVENANTS OR WARRANTIES, EITHER EXPRESSED OR IMPLIED, ORAL OR WRITTEN, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

HAND HELD PRODUCTS' RESPONSIBILITY AND PURCHASER'S EXCLUSIVE REMEDY UNDER THIS WARRANTY IS LIMITED TO THE REPAIR OR REPLACEMENT OF THE DEFECTIVE PRODUCT. IN NO EVENT SHALL HAND HELD PRODUCTS BE LIABLE FOR INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, AND, IN NO EVENT, SHALL ANY LIABILITY OF HAND HELD PRODUCTS ARISING IN CONNECTION WITH ANY PRODUCT SOLD HEREUNDER (WHETHER SUCH LIABILITY ARISES FROM A CLAIM BASED ON CONTRACT, WARRANTY, TORT, OR OTHERWISE) EXCEED THE ACTUAL AMOUNT PAID TO HAND HELD PRODUCTS FOR THE PRODUCT. THESE LIMITATIONS ON LIABILITY SHALL REMAIN IN FULL FORCE AND EFFECT EVEN WHEN HAND HELD PRODUCTS MAY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH INJURIES, LOSSES, OR DAMAGES. SOME STATES, PROVINCES, OR COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATIONS OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

All provisions of this Limited Warranty are separate and severable, which means that if any provision is held invalid and unenforceable, such determination shall not affect the validity of enforceability of the other provisions hereof.

Hand Held Products extends these warranties only to the first end-users of the products. These warranties are non-transferable.

The limited duration of the warranty for the Image Kiosk 8560 is one year.

How to Extend Your Warranty

Hand Held Products offers a variety of service plans on our hardware products. These agreements offer continued coverage for your equipment after the initial warranty expires. For more information, contact your Sales Representative, Customer Account Representative, or Product Service Marketing Manager from Hand Held Products, or your Authorized Reseller.

Hand Held Products, Inc.
700 Visions Drive
P.O. Box 208
Skaneateles Falls, NY 13153-0208